

The complexity of estimating local physical quantities

Sevag Gharibian*

Justin Yirka†

June 20, 2016

Abstract

An important task in quantum physics is the estimation of local quantities for ground states of local Hamiltonians. Recently, [Ambainis, CCC 2014] defined the complexity class $P^{QMA[\log]}$, and motivated its study by showing that the physical task of estimating the expectation value of a local observable against the ground state of a local Hamiltonian is $P^{QMA[\log]}$ -complete. (Here, $P^{QMA[\log]}$ is the set of decision problems solvable in polynomial time with access to $O(\log n)$ queries to a Quantum Merlin Arthur (QMA) oracle.) In this paper, we continue the study of $P^{QMA[\log]}$, obtaining the following results.

- The $P^{QMA[\log]}$ -completeness result of [Ambainis, CCC 2014] above requires $O(\log n)$ -local Hamiltonians and $O(\log n)$ -local observables. Whether this could be improved to the more physically appealing $O(1)$ -local setting was left as an open question. We resolve this question positively by showing that simulating even a single qubit measurement on ground states of 5-local Hamiltonians is $P^{QMA[\log]}$ -complete.
- We formalize the complexity theoretic study of estimating two-point correlation functions against ground states, and show that this task is similarly $P^{QMA[\log]}$ -complete.
- $P^{QMA[\log]}$ is thought of as “slightly harder” than QMA. We give a formal justification of this intuition by exploiting the technique of hierarchical voting of [Beigel, Hemachandra, and Wechsung, SCT 1989] to show $P^{QMA[\log]} \subseteq PP$. This improves the known containment $QMA \subseteq PP$ [Kitaev, Watrous, STOC 2000].
- A central theme of this work is the subtlety involved in the study of oracle classes in which the oracle solves a *promise* problem (such as $P^{QMA[\log]}$). In this vein, we identify a flaw in [Ambainis, CCC 2014] regarding a $P^{UQMA[\log]}$ -hardness proof for estimating spectral gaps of local Hamiltonians. By introducing a “query validation” technique, we build on [Ambainis, CCC 2014] to obtain $P^{UQMA[\log]}$ -hardness for estimating spectral gaps under polynomial-time Turing reductions.

1 Introduction

The use of computational complexity theory to study the inherent difficulty of computational problems has proven remarkably fruitful over the last decades. For example, the theory of NP-completeness [Coo72, Lev73, Kar72] has helped classify the worst-case complexity of hundreds of computational problems which elude efficient classical algorithms. In the quantum setting, the study of a quantum analogue of NP, known as Quantum Merlin Arthur (QMA), was started in 1999 by the seminal “quantum Cook-Levin theorem”

*Department of Computer Science, Virginia Commonwealth University, Richmond, VA 23284, USA. Email: sgharibian@vcu.edu. Supported by NSF grant CCF-1526189. Part of this work completed while supported by an NSERC Banting Postdoctoral Fellowship as a Simons Postdoctoral Fellow at the University of California, Berkeley.

†Department of Computer Science, Virginia Commonwealth University, Richmond, VA 23284, USA. Email: yirkajk@vcu.edu.

of Kitaev [KSV02], which showed that estimating the ground state energy of a given k -local Hamiltonian is QMA-complete for $k \geq 5$. Since then, a number of physically motivated problems have been shown complete for QMA (see, e.g., [Boo14] and [GHLS14] for surveys), a number of which focus on estimating ground state energies of local Hamiltonians.

In recent years, however, new directions in quantum complexity theory involving other physically motivated properties of local Hamiltonians have appeared. For example, Brown, Flammia and Schuch [BFS11] (see also Shi and Zhang [SZ]) introduced a quantum analogue of #P, denoted #BQP, and showed that computing the ground state degeneracy or density of states of local Hamiltonians is #BQP-complete. Gharibian and Kempe [GK12] introduced the class $\text{cq-}\Sigma_2$, a quantum generalization of Σ_2^P , and showed that determining the smallest subset of interaction terms of a given local Hamiltonian which yields a frustrated ground space is $\text{cq-}\Sigma_2$ -complete (and additionally, $\text{cq-}\Sigma_2$ -hard to approximate). Gharibian and Sikora [GS15] showed that determining whether the ground space of a local Hamiltonian has an “energy barrier” is QCMA-complete, where QCMA [AN02] is Merlin-Arthur (MA) with a classical proof and quantum prover. Finally, and most relevant to this work, Ambainis [Amb14] introduced $\text{P}^{\text{QMA}}_{[\log]}$, which is the class of decision problems decidable by a polynomial time Turing machine with logarithmically many queries to a QMA oracle (i.e. a quantum analogue of $\text{P}^{\text{NP}}_{[\log]}$). He showed that $\text{P}^{\text{QMA}}_{[\log]}$ captures the complexity of a very natural physical problem: “Simulating” a local measurement against the ground state of a local Hamiltonian (more formally, computing the expectation value of a given local observable against the ground state).

It is worth noting here that, indeed, given a local Hamiltonian, often one is not necessarily interested in a description of the *entire* ground state [GHLS14]. Rather, one may be interested in local quantities such as the evaluation of a local observable or of a correlation function. This makes $\text{P}^{\text{QMA}}_{[\log]}$ an arguably well-motivated complexity class, whose study we thus continue here.

Our results. Our findings are summarized under three headings below.

1. $\text{P}^{\text{QMA}}_{[\log]}$ -completeness for estimating local quantities. We begin with the study of two physically motivated problems. The first (discussed above), APX-SIM, was formalized by Ambainis [Amb14] and is roughly as follows (formal definitions given in Section 2): Given a k -local Hamiltonian H and an l -local observable A , estimate $\langle A \rangle := \langle \psi | A | \psi \rangle$, where $|\psi\rangle$ is a ground state of H . The second problem, which we introduce here and denote APX-2-CORR, is defined similarly to APX-SIM, except now one is given two observables A and B , and the goal is to estimate the *two-point correlation function* $\langle A \otimes B \rangle - \langle A \rangle \langle B \rangle$.

In previous work, Ambainis [Amb14] showed that APX-SIM is $\text{P}^{\text{QMA}}_{[\log]}$ -complete for $O(\log n)$ -local Hamiltonians and $O(\log n)$ -local observables. From a physical standpoint, however, it is typically desirable to have $O(1)$ -local Hamiltonians and observables, and whether $\text{P}^{\text{QMA}}_{[\log]}$ -hardness holds in this regime was left as an open question. We thus first ask: *Is APX-SIM still hard for an $O(1)$ -local Hamiltonian and 1-local observables?*

A priori, one might guess that simulating 1-local measurements might not be so difficult — for example, the ground state energy of a 1-local Hamiltonian can trivially be estimated efficiently. Yet this intuition is easily seen to be incorrect. Since one can embed a 3-SAT instance ϕ into a 3-local Hamiltonian, the ability to repeatedly locally measure observable Z against single qubits of the ground state allows one to determine a solution to ϕ ! Thus the 1-local observable case is at least NP-hard. Indeed, here we show it is much harder, resolving Ambainis’s open question in the process.

Theorem 1.1. *Given a 5-local Hamiltonian H on n qubits and a 1-local observable A , estimating $\langle A \rangle$ (i.e. APX-SIM) is $\text{P}^{\text{QMA}}_{[\log]}$ -complete.*

Thus, measuring just a *single* qubit of a local Hamiltonian H 's ground state with a fixed observable A (in our construction, A is independent of H) is harder than QMA (assuming $\text{QMA} \neq \text{P}^{\text{QMA}[\log]}$, which is likely as otherwise $\text{QMA} = \text{co-QMA}$).

Using similar techniques, we also show APX-2-CORR is $\text{P}^{\text{QMA}[\log]}$ -complete.

Theorem 1.2. *Given a 5-local Hamiltonian H on n qubits and a pair of 1-local observables A and B , estimating $\langle A \otimes B \rangle - \langle A \rangle \langle B \rangle$ (i.e. APX-2-CORR) is $\text{P}^{\text{QMA}[\log]}$ -complete.*

2. *An upper bound on the power of $\text{P}^{\text{QMA}[\log]}$.* Since $\text{P}^{\text{QMA}[\log]}$ captures the complexity of natural physical problems, and since it is thought of as “slightly harder” than QMA (and in particular, $\text{QMA} \subseteq \text{P}^{\text{QMA}[\log]}$), we next ask the question: *How much harder than QMA is $\text{P}^{\text{QMA}[\log]}$?* Recall that $\text{QMA} \subseteq \text{PP}$ [KW00, Vya03, MW05] (note [Vya03] actually shows the stronger containment $\text{QMA} \subseteq \text{A}_0\text{PP}$). Here, PP is the set of promise problems solvable in probabilistic polynomial time with *unbounded* error. Our next result shows that $\text{P}^{\text{QMA}[\log]}$ is “not too much harder” than QMA in the following rigorous sense.

Theorem 1.3. $\text{P}^{\text{QMA}[\log]} \subseteq \text{PP}$.

3. *Estimating spectral gaps and oracles for promise problems.* A central theme in this work is the subtlety involved in the study of oracle classes in which the oracle solves a *promise* problem (such as $\text{P}^{\text{QMA}[\log]}$), as opposed to a decision problem (such as $\text{P}^{\text{NP}[\log]}$, where $\text{P}^{\text{NP}[\log]}$ is defined as $\text{P}^{\text{QMA}[\log]}$ except with an NP oracle). As discussed further in “Proof techniques and discussions below”, the issue here is that a P machine *a priori* cannot in general determine if the query it makes to a QMA oracle satisfies the promise gap of the oracle. For queries which violate this promise, the oracle is allowed to give an arbitrary answer. We observe that this point appears to have been missed in [Amb14], rendering a claimed proof that determining the spectral gap of a given $O(\log n)$ -local Hamiltonian H is $\text{P}^{\text{UQMA}[\log]}$ -hard incorrect. (Here, $\text{P}^{\text{UQMA}[\log]}$ is defined as $\text{P}^{\text{QMA}[\log]}$ except with a Unique QMA oracle.) Our last result both shows how to overcome this difficulty (at the expense of obtaining a “slightly weaker” hardness claim involving a Turing reduction, whereas [Amb14] claimed hardness under a mapping reduction), and improves the locality of H to $O(1)$.

Theorem 1.4. *Given a 4-local Hamiltonian H , estimating its spectral gap (i.e. SPECTRAL-GAP) is $\text{P}^{\text{UQMA}[\log]}$ -hard under polynomial time Turing reductions (i.e. Cook reductions).*

Proof techniques and discussion.

1. *$\text{P}^{\text{QMA}[\log]}$ -completeness for estimating local quantities.* The proofs of our first two $\text{P}^{\text{QMA}[\log]}$ -hardness results (Theorem 1.1 and Theorem 1.2) are similar, so we focus on APX-SIM here. Intuitively, our aim is simple: To design our local Hamiltonian H so that its ground state encodes a so-called history state [KSV02] $|\psi\rangle$ for a given $\text{P}^{\text{QMA}[\log]}$ instance, such that measuring observable Z on the designated “output qubit” of $|\psi\rangle$ reveals the answer of the computation. At a high level, this is achieved by combining a variant of Kitaev’s circuit-to-Hamiltonian construction [KSV02] (which forces the ground state to follow the P circuit) with Ambainis’s “query Hamiltonian” [Amb14] (which forces the ground state to correspond to correctly answered queries to the QMA oracle). Making this rigorous, however, requires developing a few ideas, including: A careful analysis of Ambainis’s query Hamiltonian’s ground space when queries violating the promise gap of the oracle are allowed (Lemma 3.1; more on this below), a simple but useful corollary (Cor. 2.4) of Kempe, Kitaev, and Regev’s Projection Lemma [KKR06] (Corollary 2.4, showing that any low energy state of H must be close to a valid history state), and application of Kitaev’s unary encoding trick¹ [KSV02] to bring the locality of the Hamiltonian H down to $O(1)$ (Lemma 3.2).

¹In [KSV02], this trick was used to reduce the locality of the clock register.

Next, to show containment of APX-2-CORR in $P^{QMA[\log]}$ (Theorem 1.2), a natural approach would be to run Ambainis’s $P^{QMA[\log]}$ protocol for APX-SIM independently for each term $\langle A \otimes B \rangle$, $\langle A \rangle$, and $\langle B \rangle$. However, if a cheating prover does not send the *same* ground state $|\psi\rangle$ for each of these measurements, soundness of the protocol can be violated. To circumvent this, we exploit a trick of Chailloux and Satath [CS12] from the setting of QMA(2): we observe that the correlation function requires only knowledge of the two-body reduced density matrices $\{\rho_{ij}\}$ of $|\psi\rangle$. Thus, a prover can send classical descriptions of the $\{\rho_{ij}\}$ along with a “consistency proof” for the QMA-complete Consistency problem [Liu06].

2. *An upper bound on the power of $P^{QMA[\log]}$.* We now move to our third result, which is perhaps the most technically involved. To show $P^{QMA[\log]} \subseteq PP$ (Theorem 1.3), we exploit the technique of *hierarchical voting*, used by Beigel, Hemachandra, and Wechsung [BHW89] to show $P^{NP[\log]} \subseteq PP$, in conjunction with the QMA strong amplification results of Marriott and Watrous [MW05]. The intuition is perhaps best understood in the context of $P^{NP[\log]}$ [BHW89]. There, the PP machine first attempts to *guess* the answers to each NP query by picking random assignments to the SAT formula ϕ_i representing query i , in the hope of guessing a satisfying assignment for ϕ_i . Since such a guess can succeed only if ϕ_i is satisfiable, it can be seen that the lexicographically *largest* string y^* attainable by this process must be the correct query string (i.e. string of query answers). The scheme then uses several rounds of “hierarchical voting,” in which lexicographically smaller query strings reduce their probability of being output to the point where y^* is guaranteed to be the “most likely” query string output. While the quantum variant of this scheme which we develop is quite natural, its analysis is markedly more involved than the classical setting due to both the bounded-error nature of QMA and the possibility of “invalid queries” violating the QMA promise gap. (For example, it is no longer necessarily true that the lexicographically largest obtainable y^* is a “correct” query string.)

3. *Estimating spectral gaps and oracles for promise problems.* Finally, let us move to our fourth result and the theme of “invalid queries”. Let us assume that all calls by the $P^{QMA[\log]}$ machine to the QMA oracle Q are for an instance (H, a, b) of the Local Hamiltonian Problem (LH): Is the ground state energy of H at most a (YES case), or at least b (NO case), for $b - a \geq 1/\text{poly}(n)$? Unfortunately, a P machine cannot in general tell whether the instance (H, a, b) it feeds to Q satisfies the promise conditions of LH (i.e. the ground state energy may lie in the interval (a, b)). If the promise is violated, we call such a query *invalid*, and in this case Q is allowed to either accept or reject. This raises the issue of how to ensure a YES instance (or NO instance) of a $P^{QMA[\log]}$ problem is well-defined. To do so, we stipulate (see, e.g., Definition 3 of Goldreich [Gol06]) that the P machine must output the *same* answer regardless of how any invalid queries are answered by the oracle. As mentioned earlier, this point appears to have been missed in [Amb14], where all queries were assumed to satisfy the LH promise. This results in the proofs of two key claims of [Amb14] being incorrect. The first claim was used in the proof of $P^{QMA[\log]}$ -completeness for APX-SIM (Claim 1 in [Amb14]); we provide a corrected statement and proof in Lemma 3.1 (which suffices for the $P^{QMA[\log]}$ -hardness results in [Amb14] regarding APX-SIM to hold).

The error in the second claim (Claim 2 of [Amb14]), wherein $P^{UQMA[\log]}$ -hardness of determining the spectral gap of a local Hamiltonian is shown, appears arguably more serious. The construction of [Amb14] requires a certain “query Hamiltonian” to have a spectral gap, which indeed holds if the $P^{QMA[\log]}$ machine makes no invalid queries. However, if the machine makes invalid queries, this gap can close, and it is not clear how one can recover $P^{QMA[\log]}$ -hardness under mapping reductions. To overcome this, we introduce a technique of “query validation”, which is perhaps reminiscent of property testing: Given a query to the QMA oracle, we would like to determine if the query is valid or “far” from valid. While it is not clear how a P machine alone can solve this “property testing” problem, we show how to use a SPECTRAL GAP oracle

to do so, essentially allowing us to eliminate “sufficiently invalid” queries. Carefully combining this idea with Ambainis’s original construction [Amb14], coupled with application of Kitaev’s unary encoding trick, we show Theorem 1.4, i.e. $\text{P}^{\text{QMA}[\log]}$ -hardness for SPECTRAL-GAP for $O(1)$ -local Hamiltonians. Since our query validation approach requires a polynomial number of calls to the SPECTRAL-GAP oracle, this result requires a polynomial-time *Turing* reduction. Whether this can be improved to a mapping reduction is left as an open question.

Organization. This paper is organized as follows: In Section 2, we give notation, formal definitions, and a corollary of the Projection Lemma. In Section 3, we show various lemmas regarding Ambainis’s query Hamiltonian. In Section 4 and Section 5, we show Theorem 1.1 and Theorem 1.2, respectively. Section 6 proves Theorem 1.3. Theorem 1.4 is given in Section 7. We conclude in Section 8 and pose open questions.

2 Preliminaries

Notation. For $x \in \{0, 1\}^n$, $|x\rangle \in (\mathbb{C}^2)^{\otimes n}$ denotes the computational basis state labeled by x . Let \mathcal{X} be a complex Euclidean space. Then, $\mathcal{L}(\mathcal{X})$ and $\mathcal{D}(\mathcal{X})$ denote the sets of linear and density operators acting on \mathcal{X} , respectively. For subspace $\mathcal{S} \subseteq \mathcal{X}$, \mathcal{S}^\perp denotes the orthogonal complement of \mathcal{S} . For Hermitian operator H , $\lambda(H)$ and $\lambda(H|_{\mathcal{S}})$ denote the smallest eigenvalue of H and the smallest eigenvalue of H restricted to space \mathcal{S} , respectively. The spectral and trace norms are defined $\|A\|_\infty := \max\{\|A|v\rangle\|_2 : \|v\rangle\|_2 = 1\}$ and $\|A\|_{\text{tr}} := \text{Tr} \sqrt{A^\dagger A}$, respectively, where $:=$ denotes a definition. We set $[m] := \{1, \dots, m\}$.

Definitions and lemmas. The class PP [Gil77] is the set of promise problems for which there exists a polynomial-time probabilistic Turing machine which accepts any YES instance with probability strictly greater than $1/2$, and accepts any NO instance with probability at most $1/2$.

The class $\text{P}^{\text{QMA}[\log]}$, defined by Ambainis [Amb14], is the set of decision problems decidable by a polynomial-time deterministic Turing machine with the ability to query an oracle for a QMA-complete problem (e.g. the 2-local Hamiltonian problem (2-LH) [KKR06]) $O(\log n)$ times, where n is the size of the input. 2-LH is defined as follows: Given a 2-local Hamiltonian H and inverse polynomially separated thresholds $a, b \in \mathbb{R}$, decide whether $\lambda(H) \leq a$ (YES-instance) or $\lambda(H) \geq b$ (NO-instance). Note that the P machine is allowed to make queries which violate the promise gap of 2-LH, i.e. with $\lambda(H) \in (a, b)$; in this case, the oracle can output either YES or NO. The P machine is nevertheless required to output the same final answer (i.e. accept or reject) regardless of how such “invalid” queries are answered [Gol06].

For any P machine M making m queries to a QMA oracle, we use the following terminology throughout this article. A *valid* (*invalid*) query satisfies (violates) the promise gap of the QMA oracle. A *correct* query string $y \in \{0, 1\}^m$ encodes a sequence of correct answers to all of the m queries. Note that for any invalid query of M , any answer is considered “correct”, yielding the possible existence of multiple correct query strings. An *incorrect* query string is one which contains at least one incorrect query answer.

We now recall the definition of APX-SIM.

Definition 2.1 ($\text{APX-SIM}(H, A, k, l, a, b, \delta)$ (Ambainis [Amb14])). *Given a k -local Hamiltonian H , an l -local observable A , and real numbers a, b , and δ such that $a - b \geq n^{-c}$ and $\delta \geq n^{-c'}$, for n the number of qubits H acts on and $c, c' > 0$ some constants, decide:*

- *If H has a ground state $|\psi\rangle$ satisfying $\langle\psi| A |\psi\rangle \leq a$, output YES.*
- *If for any $|\psi\rangle$ satisfying $\langle\psi| H |\psi\rangle \leq \lambda(H) + \delta$, it holds that $\langle\psi| A |\psi\rangle \geq b$, output NO.*

Next, we briefly review Kitaev's circuit-to-Hamiltonian construction [KSV02]. Given a quantum circuit $U = U_L \cdots U_1$ consisting of 1- and 2-qubit gates U_i and acting on registers Q (proof register) and W (workspace register), this construction maps U to a 5-local Hamiltonian $H = H_{\text{in}} + H_{\text{out}} + H_{\text{prop}} + H_{\text{stab}}$. Here, we use two key properties of $H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}}$. First, the null space of $H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}}$ is spanned by *history states*, which for any $|\psi\rangle$ have form

$$|\psi_{\text{hist}}\rangle = \sum_{t=0}^L U_t \cdots U_1 |\psi\rangle_Q |0 \cdots 0\rangle_W |t\rangle_C, \quad (1)$$

where C is a clock register keeping track of time [KSV02]. Second, we use the following lower bound² on the smallest non-zero eigenvalue of $H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}}$:

Lemma 2.2 (Lemma 3 (Gharibian, Kempe [GK12])). *The smallest non-zero eigenvalue of $\Delta(H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}})$ is at least $\pi^2 \Delta / (64L^3) \in \Omega(\Delta/L^3)$, for $\Delta \in \mathbb{R}^+$ and $L \geq 1$.*

A useful fact for arbitrary complex unit vectors $|v\rangle$ and $|w\rangle$ is (see, e.g., Equation 1.33 of [Gha13]):

$$\| |v\rangle\langle v| - |w\rangle\langle w| \|_{\text{tr}} = 2\sqrt{1 - |\langle v|w\rangle|^2} \leq 2\| |v\rangle - |w\rangle \|_2. \quad (2)$$

Next, two points on complexity classes: First, let V denote a QMA verification circuit acting on M proof qubits, and with completeness c and soundness s . If one runs V on “proof” $\rho = I/2^M$, then for a YES instance, V accepts with probability at least $c/2^M$ (since $I/2^M$ can be viewed as “guessing” a correct proof with probability at least $1/2^M$), and in a NO instance, V accepts with probability at most s (see, e.g., [MW05, Wat09]). Second, the class PQP is defined analogously to BQP, except in the YES case, the verifier accepts with probability strictly larger than $1/2$, and in the NO case, the verifier accepts with probability at most $1/2$.

For clarity, throughout this article a “local” Hamiltonian is with respect to the number of qubits each local interaction term acts on, not with respect to geometric locality.

A corollary of the Projection Lemma. Finally, we show a simple but useful corollary of the Projection Lemma of Kempe, Kitaev, Regev [KKR06]

Lemma 2.3 (Kempe, Kitaev, Regev [KKR06]). *Let $H = H_1 + H_2$ be the sum of two Hamiltonians operating on some Hilbert space $\mathcal{H} = \mathcal{S} + \mathcal{S}^\perp$. The Hamiltonian H_1 is such that \mathcal{S} is a zero eigenspace and the eigenvectors in \mathcal{S}^\perp have eigenvalue at least $J > 2\|H_2\|_\infty$. Then,*

$$\lambda(H_2|_{\mathcal{S}}) - \frac{\|H_2\|_\infty^2}{J - 2\|H_2\|_\infty} \leq \lambda(H) \leq \lambda(H_2|_{\mathcal{S}}).$$

Corollary 2.4. *Let H, H_1, H_2, \mathcal{S} be as stated in Lemma 2.3, and define $K := \|H_2\|_\infty$. Then, for any $\delta \geq 0$ and vector $|\psi\rangle$ satisfying $\langle\psi|H|\psi\rangle \leq \lambda(H) + \delta$, there exists a $|\psi'\rangle \in \mathcal{S}$ such that*

$$|\langle\psi|\psi'\rangle|^2 \geq 1 - \left(\frac{K + \sqrt{K^2 + \delta(J - 2K)}}{J - 2K} \right)^2.$$

²This bound is stated as $\Omega(\Delta/L^3)$ in [GK12]; the constant $\pi^2/64$ can be derived from the analysis therein, though the exact value of the constant is not crucial in this work.

Proof. Consider arbitrary $|\psi\rangle$ such that $\langle\psi|H|\psi\rangle \leq \lambda(H) + \delta$. We can write $|\psi\rangle = \alpha_1 |\psi_1\rangle + \alpha_2 |\psi_2\rangle$ for $|\psi_1\rangle \in \mathcal{S}$, $|\psi_2\rangle \in \mathcal{S}^\perp$, $\alpha_1, \alpha_2 \in \mathbb{R}$, $\alpha_1, \alpha_2 \geq 0$, and $\alpha_1^2 + \alpha_2^2 = 1$. The proof of Lemma 2.3 yields

$$\langle\psi|H|\psi\rangle \geq \lambda(H_2|_{\mathcal{S}}) + (J - 2K)\alpha_2^2 - 2K\alpha_2. \quad (3)$$

For completeness, we reproduce the steps from [KKR06] to derive this inequality as follows:

$$\begin{aligned} \langle\psi|H|\psi\rangle &\geq \langle\psi|H_2|\psi\rangle + J\alpha_2^2 \\ &= (1 - \alpha_2^2) \langle v_1|H_2|v_1\rangle + 2\alpha_1\alpha_2 \operatorname{Re} \langle\psi_1|H_2|\psi_2\rangle + \\ &\quad \alpha_2^2 \langle\psi_2|H_2|\psi_2\rangle + J\alpha_2^2 \\ &\geq \langle v_1|H_2|v_1\rangle - K(\alpha_2^2 + 2\alpha_2 + \alpha_2^2) + J\alpha_2^2 \\ &= \langle v_1|H_2|v_1\rangle + (J - 2K)\alpha_2^2 - 2K\alpha_2 \\ &\geq \lambda(H_2|_{\mathcal{S}}) + (J - 2K)\alpha_2^2 - 2K\alpha_2. \end{aligned}$$

Since by assumption $\langle\psi|H|\psi\rangle \leq \lambda(H) + \delta$, Equation (3) implies $\lambda(H) + \delta \geq \lambda(H_2|_{\mathcal{S}}) + (J - 2K)\alpha_2^2 - 2K\alpha_2$. Combining this with Lemma 2.3, we have

$$0 \geq \lambda(H) - \lambda(H_2|_{\mathcal{S}}) \geq (J - 2K)\alpha_2^2 - 2K\alpha_2 - \delta,$$

which holds only if $|\alpha_2| \leq \frac{K + \sqrt{K^2 + \delta(J - 2K)}}{J - 2K}$. Thus, setting $|\psi'\rangle = |\psi_1\rangle$ yields the claim. \square

3 Ambainis's Query Hamiltonian

In this section, we show various results regarding Ambainis's "query Hamiltonian" [Amb14], which intuitively aims to have its ground space contain correct answers to a sequence of QMA queries. Let U be a $\text{PQMA}^{\text{[log]}}$ computation, and let $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$ be the 2-local Hamiltonian corresponding to the i th query made by U given that the answers to the previous $i - 1$ queries are given by $y_1 \dots y_{i-1}$. (Without loss of generality, we may assume $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}} \succeq 0$ by adding multiples of the identity and rescaling.) The oracle query made at step i corresponds to an input $(H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}, \epsilon, 3\epsilon)$ to 2-LH, for $\epsilon > 0$ a fixed inverse polynomial. Then, Ambainis's [Amb14] $O(\log(n))$ -local query Hamiltonian H acts on $\mathcal{X} \otimes \mathcal{Y}$, where $\mathcal{X} = (\mathcal{X}_i)^{\otimes m} = (\mathbb{C}^2)^{\otimes m}$ and $\mathcal{Y} = \otimes_{i=1}^m \mathcal{Y}_i$, such that \mathcal{X}_i is intended to encode the answer to query i with \mathcal{Y}_i encoding the ground state of the corresponding query Hamiltonian $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$. Specifically,

$$\begin{aligned} H &= \sum_{i=1}^m \frac{1}{4^{i-1}} \sum_{y_1, \dots, y_{i-1}} \bigotimes_{j=1}^{i-1} |y_j\rangle\langle y_j|_{\mathcal{X}_j} \otimes \left(2\epsilon |0\rangle\langle 0|_{\mathcal{X}_i} \otimes I_{\mathcal{Y}_i} + |1\rangle\langle 1|_{\mathcal{X}_i} \otimes H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}} \right) \\ &=: \sum_{i=1}^m \frac{1}{4^{i-1}} \sum_{y_1, \dots, y_{i-1}} M_{y_1 \dots y_{i-1}}. \end{aligned} \quad (4)$$

Recall from Section 2 that we call a sequence of query answers $y = y_1 \dots y_m \in \{0, 1\}^m$ *correct* if it corresponds to a possible execution of U . Since U can make queries to its QMA oracle which violate the QMA promise gap, the set of correct y is generally not a singleton. However, we henceforth assume without loss of generality that U makes at least one valid query (i.e. which satisfies the QMA promise gap). For if not, then a P machine can solve such an instance by simulating the $\text{PQMA}^{\text{[log]}}$ machine on all possible (polynomially many) query strings $y \in \{0, 1\}^m$. If U corresponds to a YES (NO) instance, then *all* query strings lead to accept (reject), which the P machine can verify.

We now prove the following about H .

Lemma 3.1. *Define for any $x \in \{0, 1\}^m$ the space $\mathcal{H}_{x_1 \dots x_m} := \bigotimes_{i=1}^m |x_i\rangle\langle x_i| \otimes \mathcal{Y}_i$. Then, there exists a correct query string $x \in \{0, 1\}^m$ such that the ground state of H lies in $\mathcal{H}_{x_1 \dots x_m}$. Moreover, suppose this space has minimum eigenvalue λ . Then, for any incorrect query string $y_1 \dots y_m$, any state in $\mathcal{H}_{y_1 \dots y_m}$ has energy at least $\lambda + \frac{\epsilon}{4^m}$.*

As discussed in Section 1, Claim 1 of [Amb14] proved a similar statement under the assumption that the correct query string x is unique. In that setting, [Amb14] showed that the ground state of H is in \mathcal{H}_x , and that for *all* other query strings $y \neq x$, the space \mathcal{H}_y has energy at least $\lambda + \frac{\epsilon}{4^{m-1}}$. However, in general invalid queries must be allowed, and in this setting this claim no longer holds — two distinct correct query strings can have eigenvalues which are arbitrarily close if they contain queries violating the promise gap. The key observation we make here is that even in the setting of non-unique x , a spectral gap between the ground space and all *incorrect* query strings can be shown, which suffices for our purposes. (In other words, note that Lemma 3.1 does not yield a spectral gap between λ and the minimum eigenvalue in spaces $\mathcal{H}_{y_1 \dots y_m}$ for correct query strings $y \neq x$.)

Proof of Lemma 3.1. Observe first that H in Equation (4) is block-diagonal with respect to register \mathcal{X} , i.e. to understand the spectrum of H , it suffices to understand the eigenvalues in each of the blocks corresponding to fixing \mathcal{X}_i to some string $y \in \{0, 1\}^m$. Thus, we can restrict our attention to spaces \mathcal{H}_y for $y \in \{0, 1\}^m$. To begin, let $x \in \{0, 1\}^m$ denote a correct query string which has lowest energy among all *correct* query strings against H , i.e. the block corresponding to x has the smallest eigenvalue among such blocks. (Note that x is well-defined, though it may not be unique; in this latter case, any such x will suffice for our proof.) For any $y \in \{0, 1\}^m$, define λ_y as the smallest eigenvalue in block \mathcal{H}_y . We show that for any *incorrect* query string $y = y_1 \dots y_m$, $\lambda_y \geq \lambda_x + \epsilon/(4^m)$.

We use proof by contradiction, coupled with an exchange argument. Suppose there exists an incorrect query string $y = y_1 \dots y_m$ such that $\lambda_y < \lambda_x + \epsilon/(4^m)$. Since y is an incorrect query string, there exists an $i \in [m]$ such that y_i is the wrong answer to a valid query $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$. Let i denote the first such position. Now, consider operator $M_{y_1 \dots y_{i-1}}$, which recall is defined as

$$M_{y_1 \dots y_{i-1}} = \bigotimes_{j=1}^{i-1} |y_j\rangle\langle y_j|_{\mathcal{X}_j} \otimes \left(2\epsilon |0\rangle\langle 0|_{\mathcal{X}_i} \otimes I_{\mathcal{Y}_i} + |1\rangle\langle 1|_{\mathcal{X}_i} \otimes H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}} \right)$$

and let $\lambda_{y_1 \dots y_{i-1} \bar{y}_i}$ denote the smallest eigenvalue of $M_{y_1 \dots y_{i-1}}$ restricted to space $\mathcal{H}_{y_1 \dots y_{i-1} \bar{y}_i}$, where string $y_1 \dots y_{i-1} \bar{y}_i$ is a correct query string with \bar{y}_i the correct answer to query i . Then, any state $|\phi\rangle \in \mathcal{H}_{y_1 \dots y_i}$ satisfies

$$\langle \phi | M_{y_1 \dots y_{i-1}} | \phi \rangle \geq \lambda_{y_1 \dots y_{i-1} \bar{y}_i} + \epsilon/4^{i-1}. \quad (5)$$

This is because constrained to space $\mathcal{H}_{y_1 \dots y_{i-1}}$, $M_{y_1 \dots y_{i-1}}$ reduces to operator $M' := 2\epsilon |0\rangle\langle 0|_{\mathcal{X}_i} \otimes I_{\mathcal{Y}_i} + |1\rangle\langle 1|_{\mathcal{X}_i} \otimes H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$. If query i is a YES-instance, the smallest eigenvalue of M' lies in the block corresponding to setting \mathcal{X}_i to (the correct query answer) $|1\rangle$, and is at most ϵ . On the other hand, the block with \mathcal{X}_i set to $|0\rangle$ has all eigenvalues equalling 2ϵ . A similar argument shows that in the NO-case, the $|0\rangle$ -block has eigenvalues equalling 2ϵ , and the $|1\rangle$ -block has eigenvalues at least 3ϵ . Combining this with the $1/4^{i-1}$ factor in Equation (4) yields Equation (5). We conclude that flipping query bit i to the correct query answer \bar{y}_i allows us to choose an assignment from $\mathcal{H}_{y_1 \dots y_{i-1} \bar{y}_i}$ so that we “save” an energy penalty of $\epsilon/4^{i-1}$ against $M_{y_1, \dots, y_{i-1}}$.

To complete the exchange argument, let $\widehat{M}_{y_1 \dots y_t}$ denote the set of terms from Equation (4) which are consistent with prefix $y_1 \dots y_t$ (e.g. $M_{y_1 \dots y_t}$, $M_{y_1 \dots y_t 0}$, $M_{y_1 \dots y_t 1}$, etc). Fix each of the bits $y_{i+1} \dots y_m$ to a

new tail of bits $y'_{i+1} \cdots y'_m$ so that $y' := y_1 \cdots \bar{y}_i y'_{i+1} \cdots y'_m$ is a correct query string. Care is required here; the new query bits $y'_{i+1} \cdots y'_m$ may lead to different energy penalties than the previous string $y_{i+1} \cdots y_m$ against the Hamiltonian terms in set $\widehat{M}_{y_1 \cdots \bar{y}_i}$. In other words, we must upper bound any possible energy penalty *increase* when mapping $y_1 \cdots \bar{y}_i y_{i+1} \cdots y_m$ to y' . To do so, recall that all Hamiltonian terms in Equation (4) are positive semidefinite. Thus, for any state $|\psi\rangle$ in space $\mathcal{H}_{y_1 \cdots \bar{y}_i}$, the energy obtained by $|\psi\rangle$ against terms in $\widehat{M}_{y_1 \cdots \bar{y}_i}$ is at least 0. Conversely, in the worst case, since each term in $\widehat{M}_{y_1 \cdots \bar{y}_i}$ has minimum eigenvalue at most 2ϵ , the eigenvector $|\psi\rangle$ of smallest eigenvalue in block $H_{y'}$ incurs an additional penalty for queries $i+1$ through m of at most

$$2\epsilon \sum_{k=i}^{\infty} \frac{1}{4^k} = \frac{2\epsilon}{3 \cdot 4^{i-1}}.$$

We conclude that

$$\lambda_{y'} \leq \lambda_y - \frac{\epsilon}{4^{i-1}} + \frac{2\epsilon}{3 \cdot 4^{i-1}} < \left(\lambda_x + \frac{\epsilon}{4^m} \right) - \frac{\epsilon}{4^{i-1}} + \frac{2\epsilon}{3 \cdot 4^{i-1}} < \lambda_x$$

where the first inequality follows by the assumption $\lambda_y < \lambda_x + \epsilon/4^m$. This is a contradiction. \square

Our next step is to convert H from an $O(\log n)$ -local Hamiltonian to an $O(1)$ -local one.

Lemma 3.2. *For any $x \in \{0, 1\}^m$, let \hat{x} denote its unary encoding. Then, for any $\text{PQMA}^{[\log]}$ circuit U acting on n bits and making $m \geq 1$ queries to a QMA oracle, there exists a mapping to a 4-local Hamiltonian H' acting on space $(\mathbb{C}^2)^{\otimes 2^m-1} \otimes \mathcal{Y}$ such that there exists a correct query string $x = x_1 \cdots x_m$ satisfying:*

1. *The ground state of H' lies in subspace $|\hat{x}\rangle\langle\hat{x}| \otimes \mathcal{Y}$.*
2. *For any state $|\psi\rangle$ in subspace $|\hat{x}'\rangle\langle\hat{x}'| \otimes \mathcal{Y}$ where either \hat{x}' is not a unary encoding of a binary string x' or x' is an incorrect query string, one has $\langle\psi| H' |\psi\rangle \geq \lambda(H') + \epsilon/4^m$, for inverse polynomial ϵ .*
3. *For all strings $x' \in \{0, 1\}^m$, H' acts invariantly on subspace $|\hat{x}'\rangle\langle\hat{x}'| \otimes \mathcal{Y}$.*
4. *The mapping can be computed in time polynomial in n (recall $m \in O(\log n)$).*

Proof. We show how to improve the $O(\log(n))$ -local construction H of Lemma 3.1 to 4-local H' . Specifically, recall that H from Equation (4) acts on $(\mathcal{X} \otimes \mathcal{Y})$. Using a trick of Kitaev [KSV02], we encode the $\mathcal{X} = \mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m$ register in unary. Specifically, we can write

$$\begin{aligned} M_{y_1 \cdots y_{i-1}} &= \sum_{y_{i+1}, \dots, y_m} 2\epsilon \bigotimes_{j=1}^{i-1} |y_j\rangle\langle y_j|_{\mathcal{X}_j} \otimes |0\rangle\langle 0|_{\mathcal{X}_i} \bigotimes_{k=i+1}^m |y_k\rangle\langle y_k|_{\mathcal{X}_k} \otimes I_{\mathcal{Y}} + \\ &\quad \bigotimes_{j=1}^{i-1} |y_j\rangle\langle y_j|_{\mathcal{X}_j} \otimes |1\rangle\langle 1|_{\mathcal{X}_i} \bigotimes_{k=i+1}^m |y_k\rangle\langle y_k|_{\mathcal{X}_k} \otimes H_{\mathcal{Y}_i}^{i, y_1 \cdots y_{i-1}}. \end{aligned}$$

We now replace register $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m$ with register $\mathcal{X}' = (\mathbb{C}^2)^{\otimes 2^m-1}$ and encode each binary string $x \in \{0, 1\}^m$ as the unary string $\hat{x} = |1\rangle^{\otimes |x|} |0\rangle^{\otimes 2^m-|x|-1}$, where $|x|$ is the non-negative integer corresponding to string x . In other words, for $M_{x_1 \cdots x_{i-1}}$, we replace each string $|x\rangle\langle x|_{\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m}$ with $|1\rangle\langle 1|_{\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_{|x|}} \otimes |0\rangle\langle 0|_{\mathcal{X}_{|x|+1} \otimes \cdots \otimes \mathcal{X}_{2^m-1}}$. Denote the resulting Hamiltonian as H_1 .

To ensure states in \mathcal{X}' follow this encoding, add a weighted version of Kitaev's [KSV02] penalty Hamiltonian,

$$H_{\text{stab}} = 3\epsilon \sum_{j=1}^{2^m-2} |0\rangle\langle 0|_j \otimes |1\rangle\langle 1|_{j+1},$$

i.e., our final Hamiltonian is $H' = H_1 + H_{\text{stab}}$. To show that H' satisfies the same properties as H as stated in the claim, we follow the analysis of Kitaev [KSV02]. Namely, partition the space $\mathcal{X}' \otimes \mathcal{Y}$ into orthogonal spaces \mathcal{S} and \mathcal{S}^\perp corresponding to the space of valid and invalid unary encodings of \mathcal{X}' , respectively. Since H_1 and H_{stab} act invariantly on \mathcal{S} and \mathcal{S}^\perp , we can consider \mathcal{S} and \mathcal{S}^\perp separately. In \mathcal{S} , H' is identical to H , implying the claim. In \mathcal{S}^\perp , the smallest non-zero eigenvalue of H_{stab} is at least 3ϵ . Thus, since $H_1 \succeq 0$, if we can show that the smallest eigenvalue of H is at most $3\epsilon - \epsilon/4^m$, we have shown the claim (since, in particular, we will have satisfied statement 2 of our claim). To show this bound on the smallest eigenvalue, suppose x is all zeroes, i.e. set register $\mathcal{X}_1 \otimes \cdots \otimes \mathcal{X}_m$ for H to all zeroes. Then, each term $M_{0_1 \dots 0_{i-1}}$ yields an energy penalty of exactly 2ϵ , yielding an upper bound on the smallest eigenvalue of H of $2\epsilon \sum_{k=0}^{m-1} \frac{1}{4^k} \leq \frac{8}{3}\epsilon = 3\epsilon - \epsilon/3$. \square

4 Measuring 1-local observables

We now restate and prove Theorem 1.1.

Theorem 1.1. *APX-SIM is $\text{P}^{\text{QMA}[\log]}$ -complete for $k = 5$ and $l = 1$, i.e., for 5-local Hamiltonian H and 1-local observable A .*

Proof. Containment in $\text{P}^{\text{QMA}[\log]}$ was shown for $k, l \in O(\log n)$ in [Amb14]; we show $\text{P}^{\text{QMA}[\log]}$ -hardness here. Let U' be an arbitrary $\text{P}^{\text{QMA}[\log]}$ circuit corresponding to instance Π , such that U' acts on workspace register W and query result register Q . Suppose U' consists of L' gates and makes $m = c \log(n)$ queries, for $c \in O(1)$ and n the input size. Without loss of generality, U' can be simulated with a similar unitary U which treats Q as a *proof* register which it does not alter at any point: Namely, U does not have access to a QMA oracle, but rather reads bit Q_i whenever it desires the answer to the i th query. Thus, if a correct query string $y_1 \cdots y_m$ corresponding to an execution of U' on input x is provided in Q as a “proof”, then the output statistics of U' and U are identical. We can also assume without loss of generality that Q is encoded not in binary, but in unary. Thus, Q consists of $2^m - 1 \in \text{poly}(n)$ bits. For simplicity in our discussion, however, we will continue to speak of m -bit query strings $y = y_1 \cdots y_m$ in register Q .

Next, we map U to a 5-local Hamiltonian H_1 via a modification of the circuit-to-Hamiltonian construction of Kitaev [KSV02], such that H_1 acts on registers W (workspace register), Q (proof register), and C (clock register). Recall from Section 2 that Kitaev's construction outputs Hamiltonian terms $H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}} + H_{\text{out}}$. Set $H_1 = \Delta(H_{\text{in}} + H_{\text{prop}} + H_{\text{stab}})$ for Δ to be set as needed. It is crucial that H_{out} be omitted from H_1 , as we require our final Hamiltonian H to enforce a certain structure on the ground space *regardless* of whether the computation should accept or reject. The job of “checking the output” is instead delegated to the observable A . More formally, note that H_1 has a non-trivial null space, which is its ground space, consisting of history states $|\psi_{\text{hist}}\rangle$ (Equation (1)) which simulate U on registers W and Q . These history states correctly simulate U' assuming that Q is initialized to a correct proof.

To thus enforce that Q be initialized to a correct proof, let H_2 be our variant of Ambainis's query Hamiltonian from Lemma 3.2, such that H_2 acts on registers Q and Q' (where for clarity $Q = (\mathbb{C}^2)^{\otimes 2^m-1}$ (recall $m \in O(\log n)$) and $Q' = \mathcal{Y}$ from Lemma 3.2). Hence, our final Hamiltonian is $H = H_1 + H_2$, which is 5-local since H_1 is 5-local. Suppose without loss of generality that U 's output qubit is W_1 , which

is set to $|0\rangle$ until the final time step, in which the correct output is copied to it. Then, set observable $A = (I + Z)/2$ such that A acts on qubit W_1 . Set $a = 1 - 1/(L + 1)$, and $b = 1 - 1/2L$ for L the number of gates in U . Fix $\eta \geq \max(\|H_2\|_\infty, 1)$ (such an η can be efficiently computed by applying the triangle inequality and summing the spectral norms of each term of H_2 individually). Set $\Delta = L^3\eta\gamma$ for γ a monotonically increasing polynomial function of L to be set as needed. Finally, set $\delta = 1/\Delta$. This completes the construction.

Correctness. Suppose Π is a YES instance. Then, by Lemma 3.2, the ground space of H_2 is the span of states of the form $|\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$, where \hat{x} is a correct query string encoded in unary. Fix an arbitrary such ground state $|\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$. Note that setting Q to \hat{x} in this manner causes U to accept with certainty. Consider the history state $|\psi_{\text{hist}}\rangle$ on registers W , C , Q , and Q' (Q and Q' together are the “proof register”, and the contents of Q' are not accessed by U), which lies in the ground space of H_1 . Since U can read but does not alter the contents of Q , the history state has the tensor product form $|\psi'_{\text{hist}}(x)\rangle_{W,C} \otimes |\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$ for some $|\psi'_{\text{hist}}(x)\rangle_{W,C}$, i.e. the action of H_2 on the history state is unaffected. We conclude that $|\psi'_{\text{hist}}(x)\rangle_{W,C} \otimes |\hat{x}\rangle_Q \otimes |\phi\rangle_{Q'}$ is in the ground space of H . Moreover, since U accepts \hat{x} , the expectation of this state against A is $1 - 1/(L + 1)$.

Conversely, suppose we have a NO instance Π , and consider any $|\psi\rangle$ satisfying $\langle\psi|H|\psi\rangle \leq \lambda(H) + \delta$. By Lemma 2.2, the smallest non-zero eigenvalue of ΔH_1 is at least $J = \pi^2\Delta/(64L^3) = \pi^2\eta\gamma/64$. Recalling that $\delta = 1/\Delta$, apply Corollary 2.4 to obtain that there exists a valid history state $|\psi'\rangle$ on W , C , Q , and Q' such that $|\langle\psi|\psi'\rangle|^2 \geq 1 - O(\gamma^{-2}L^{-6})$, which by Equation (2) implies

$$\| |\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'| \|_{\text{tr}} \leq \frac{c}{\gamma L^3} \quad (6)$$

for some constant $c > 0$. By definition, such a history state $|\psi'\rangle$ simulates U given “quantum proof” $|\phi\rangle_{Q,Q'}$ in registers Q and Q' , i.e. $|\psi'\rangle = \sum_t U_t \cdots U_1 |0 \cdots 0\rangle_W |t\rangle_C |\phi\rangle_{Q,Q'}$. By Equation (6) and the Hölder inequality,

$$|\text{Tr}(H |\psi\rangle\langle\psi|) - \text{Tr}(H |\psi'\rangle\langle\psi'|)| \leq \frac{c}{\gamma L^3} \|H\|_\infty =: \gamma'.$$

Thus, $\langle\psi'|H|\psi'\rangle \leq \lambda(H) + (\delta + \gamma')$.

We now analyze the structure of $|\phi\rangle_{Q,Q'}$. By Lemma 3.2, the ground space \mathcal{G} of H_2 is contained in the span of states of the form $|\hat{x}\rangle_Q \otimes |\phi'\rangle_{Q'}$ where \hat{x} is a correct query string encoded in unary. Since the ground spaces of H_1 and H_2 have non-empty intersection, i.e. history states acting on “quantum proofs” from \mathcal{G} (which lie in the null space of H_1 and obtain energy $\lambda(H_2)$ against H_2), we know $\lambda(H) = \lambda(H_2)$. Thus, since $H_1 \succeq 0$,

$$\langle\psi'|H_2|\psi'\rangle \leq \langle\psi'|H|\psi'\rangle \leq \lambda(H_2) + (\delta + \gamma'). \quad (7)$$

Write $|\phi\rangle = \alpha|\phi_1\rangle + \beta|\phi_2\rangle$ for $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$ and for unit vectors

$$\begin{aligned} |\phi_1\rangle &\in \text{Span} \{ |\hat{x}\rangle_Q \otimes |\phi'\rangle_{Q'} \mid \text{correct query string } x \}, \\ |\phi_2\rangle &\in \text{Span} \{ |\hat{x}\rangle_Q \otimes |\phi'\rangle_{Q'} \mid \text{incorrect query string } x \}. \end{aligned}$$

Since any history state $|\psi'\rangle$, for any amplitudes α_x and unit vectors $|\phi'_x\rangle$, has the form

$$|\psi'\rangle = \sum_{t,x} \alpha_x U_t \cdots U_1 |0 \cdots 0\rangle_W |t\rangle_C |\hat{x}\rangle_Q |\phi'_x\rangle_{Q'} = \sum_x \alpha_x |\psi'_{\text{hist}}(x)\rangle_{W,C} |\hat{x}\rangle_Q |\phi'_x\rangle_{Q'}$$

(i.e. for any fixed x , $|\hat{x}\rangle_Q$ is not altered), and since H_2 is block-diagonal with respect to strings in Q , by Equation (7) and Lemma 3.2 we have

$$\begin{aligned}\lambda(H_2) + (\delta + \gamma') &\geq \langle \psi' | H_2 | \psi' \rangle \\ &= |\alpha|^2 \langle \phi_1 | H_2 | \phi_1 \rangle + |\beta|^2 \langle \phi_2 | H_2 | \phi_2 \rangle \\ &\geq |\alpha|^2 \lambda(H_2) + |\beta|^2 \left(\lambda(H_2) + \frac{\epsilon}{4^m} \right),\end{aligned}$$

which implies $|\beta|^2 \leq 4^m(\delta + \gamma')/\epsilon$. Thus, defining $|\psi''\rangle$ as the history state for “proof” $|\phi_1\rangle_{Q,Q'}$, we have that $\| |\psi\rangle\langle\psi| - |\psi''\rangle\langle\psi''| \|_{\text{tr}}$ is at most

$$\| |\psi\rangle\langle\psi| - |\psi'\rangle\langle\psi'| \|_{\text{tr}} + \| |\phi\rangle\langle\phi| - |\phi_1\rangle\langle\phi_1| \|_{\text{tr}} \leq \frac{c}{\gamma L^3} + 2\sqrt{\frac{4^m(\delta + \gamma')}{\epsilon}}, \quad (8)$$

which follows from the triangle inequality and the structure of the history state. Observe now that increasing γ by a polynomial factor decreases $\delta + \gamma'$ by a polynomial factor. Thus, set γ as a large enough polynomial in L such that

$$\frac{c}{\gamma L^3} + 2\sqrt{\frac{4^m(\delta + \gamma')}{\epsilon}} \leq \frac{1}{2L}. \quad (9)$$

Since U rejects any correct query string (with certainty) in the NO case, and since $|\psi''\rangle$ is a valid history state whose Q register is a superposition over correct query strings (all of which must lead to reject), we conclude that $\langle \psi'' | A | \psi'' \rangle = 1$. Moreover,

$$|\text{Tr}(A |\psi\rangle\langle\psi|) - \text{Tr}(A |\psi''\rangle\langle\psi''|)| \leq \|A\|_\infty \| |\psi\rangle\langle\psi| - |\psi''\rangle\langle\psi''| \|_{\text{tr}} \leq \frac{1}{2L},$$

where the first inequality follows from Hölder’s inequality, and the second by Equations (8) and (9). We conclude that $\langle \psi | A | \psi \rangle \geq 1 - 1/(2L)$, completing the proof. \square

5 Estimating two-point correlation functions

We now define APX-2-CORR and show that it is $\text{PQMA}^{[\log]}$ -complete using similar techniques to Section 4. For brevity, define $f(|\psi\rangle, A, B) := \langle \psi | A \otimes B | \psi \rangle - \langle \psi | A | \psi \rangle \langle \psi | B | \psi \rangle$.

Definition 5.1 (APX-2-CORR($H, A, B, k, l, a, b, \delta$)). *Given a k -local Hamiltonian H , l -local observables A and B , and real numbers a, b , and δ such that $a - b \geq n^{-c}$ and $\delta \geq n^{-c'}$, for n the number of qubits H acts on and $c, c' \geq 0$ some constants, decide:*

- If H has a ground state $|\psi\rangle$ satisfying $f(|\psi\rangle, A, B) \geq a$, output YES.
- If for any $|\psi\rangle$ satisfying $\langle \psi | H | \psi \rangle \leq \lambda(H) + \delta$ it holds that $f(|\psi\rangle, A, B) \leq b$, output NO.

We now prove Thm 1.2 by showing $\text{PQMA}^{[\log]}$ -hardness in Lemma 5.2 and containment in $\text{PQMA}^{[\log]}$ in Lemma 5.3.

Lemma 5.2. *APX-2-CORR is $\text{PQMA}^{[\log]}$ -hard for $k = 5$ and $l = 1$, i.e., for 5-local Hamiltonian H and 1-local observables A and B .*

Proof. For an arbitrary $\text{PQMA}^{\text{[log]}}$ circuit U' , define U as in the proof of Theorem 1.1, consisting of L one- and two-qubit gates. We modify U as follows. Let U 's output qubit be denoted W_1 . We add two ancilla qubits, W_2 and W_3 , which are set to $|00\rangle$ throughout U 's computation. We then append to U a sequence of six 2-qubit gates which, controlled on W_1 , map $|00\rangle$ in W_2W_3 to $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, e.g. apply a controlled Hadamard gate and the 5-gate Toffoli construction from Figure 4.7 of [NC00]. Appending six identity gates on W_1 , we obtain a circuit $V = V_{L+12} \cdots V_1$ which has $L + 12$ gates. Finally, we construct $H = H_1 + H_2$ as in the proof of Theorem 1.1, mapping V to a 5-local Hamiltonian H_1 on registers W , Q , and C , and we set $A = Z_{W_2}$ and $B = Z_{W_3}$ for Pauli Z . Similar to the proof of Theorem 1.1, set $\Delta = L^3\eta\gamma$ and $\delta = 1/\Delta$, for γ large enough so that

$$\frac{c}{\gamma L^3} + 2\sqrt{\frac{4^m(\delta + \gamma')}{\epsilon}} \leq \frac{1}{2(L + 13)}, \quad (10)$$

for γ' as defined in the proof of Theorem 1.1. Set $a = 3/(L + 13)$ and $b = 1/(L + 13)$. This completes the construction.

To set up the correctness proof, consider history state $|\psi_{\text{hist}}\rangle$ for V given quantum proof $|\phi\rangle_{Q,Q'}$, and define for brevity $|\phi_t\rangle := V_t \cdots V_1 |\phi\rangle_{Q,Q'} |0 \cdots 0\rangle_W |00\rangle_{W_2W_3}$. Then,

$$\langle \psi_{\text{hist}} | Z_{W_2} \otimes Z_{W_3} | \psi_{\text{hist}} \rangle = \frac{1}{L + 13} \sum_{t=0}^{L+12} \text{Tr} \left((|\phi_t\rangle\langle\phi_t|_{Q,Q',W} \otimes |t\rangle\langle t|_C) Z_{W_2} \otimes Z_{W_3} \right), \quad (11)$$

since $Z_{W_2} \otimes Z_{W_3}$ acts invariantly on the clock register. Defining $|v\rangle := \sum_{t=L+1}^{L+12} |\phi_t\rangle_{Q,Q',W} |t\rangle_C$, we have that since W_2W_3 is set to $|00\rangle$ for times $0 \leq t \leq L$, Equation (11) simplifies to $((L + 1) + \langle v | Z_{W_2} \otimes Z_{W_3} | v \rangle) / (L + 13)$. Thus, via similar reasoning $f(|\psi_{\text{hist}}\rangle, Z_{W_2}, Z_{W_3})$ equals

$$\frac{1}{L + 13} [(L + 1) + \langle v | Z_{W_2} \otimes Z_{W_3} | v \rangle] - \frac{1}{(L + 13)^2} [(L + 1) + \langle v | Z_{W_2} | v \rangle] [(L + 1) + \langle v | Z_{W_3} | v \rangle]. \quad (12)$$

Suppose now that Π is a YES instance. Then there exists a history state $|\psi_{\text{hist}}\rangle$ in the ground space of H (i.e. with quantum proof $|\phi\rangle_{Q,Q'} = |\hat{x}\rangle_Q \otimes |\phi'\rangle_{Q'}$ for a correct query string x) for which W_2W_3 is set to $|\phi^+\rangle$ in the final seven timesteps (since U' is deterministic). Since $\langle \phi^+ | Z \otimes Z | \phi^+ \rangle = 1$ and $\langle \phi^+ | Z \otimes I | \phi^+ \rangle = 0$, we can lower bound Equation (12) by

$$\frac{(L + 1) - 5 + 7}{L + 13} - \frac{((L + 1) + 5)^2}{(L + 13)^2} = \frac{1}{L + 13} \left(4 - \frac{49}{L + 13} \right),$$

where the ± 5 terms correspond to timesteps $t = L + 1, \dots, L + 5$ and use the fact that $\|Z\|_\infty = 1$.

Conversely, suppose Π is a NO instance, and consider any $|\psi\rangle$ satisfying $\langle \psi | H | \psi \rangle \leq \lambda(H) + \delta$. Then, as argued in the proof of Theorem 1.1, there exists a history state $|\psi''\rangle$ on “proof” $|\phi_1\rangle_{Q,Q'}$ (consisting of a superposition of correct query strings) satisfying $\| |\psi\rangle\langle\psi| - |\psi''\rangle\langle\psi''| \|_{\text{tr}} \leq (2(L + 13))^{-1}$, by Equations (8), (9) and (10). Since the history state $|\psi''\rangle$ has W_2W_3 set to $|00\rangle$ in all time steps, using Equation (12) and applying the Hölder inequality to each term of $f(|\psi\rangle, Z_{W_2}, Z_{W_3})$ yields upper bound

$$1 - \left(1 - \frac{1}{2(L + 13)} \right)^2 = \frac{1}{L + 13} \left(1 - \frac{1}{4(L + 13)} \right).$$

□

Lemma 5.3. APX-2-CORR is in $\text{PQMA}^{\text{[log]}}$.

Proof. The proof combines ideas from Ambainis’s original proof of $\text{APX-SIM} \in \text{PQMA}^{\text{[log]}}$ [Amb14] (see Theorem 6 therein) and a trick of Chailloux and Sattath [CS12] from the study of $\text{QMA}(2)$. We give a proof sketch here. Specifically, let $\Pi = (H, A, B, k, l, a, b, \delta)$ be an instance of APX-2-CORR . Similar to [Amb14], the $\text{PQMA}^{\text{[log]}}$ verification procedure proceeds, at a high level, as follows:

1. Use logarithmically many QMA oracle queries to perform a binary search to obtain an estimate $\gamma \in \mathbb{R}$ satisfying $\lambda(H) \in [\gamma, \gamma + \frac{\delta}{2}]$.
2. Use a single QMA oracle query to verify the statement: “There exists $|\psi\rangle$ satisfying (1) $\langle\psi|H|\psi\rangle \leq \lambda(H) + \delta$ and (2) $f(|\psi\rangle, A, B) \geq a$.”

The first of these steps is performed identically to the proof of $\text{APX-SIM} \in \text{PQMA}^{\text{[log]}}$ [Amb14]; we do not elaborate further here. The second step, however, differs from [Amb14] for the following reason. Intuitively, [Amb14] designs a QMA protocol which takes in many copies of a proof $|\psi\rangle$, performs phase estimation on each copy, postselects to “snap” each copy of $|\psi\rangle$ into a low-energy state $|\psi_i\rangle$ of H , and subsequently uses states $\{|\psi_i\rangle\}$ to estimate the expectation against an observable A . If the ground space of H is degenerate, the states $\{|\psi_i\rangle\}$ may not all be identical. This does not pose a problem in [Amb14], as there soundness of the protocol is guaranteed since all low energy states have high expectation against A . In our setting, however, if we use this protocol to individually estimate each of the terms $\langle\psi|A \otimes B|\psi\rangle$, $\langle\psi|A|\psi\rangle$, and $\langle\psi|B|\psi\rangle$, soundness *can* be violated if each of these three terms are not estimated using the same state $|\psi_i\rangle$, since the promise gap of the input does not necessarily say anything about the values of each of these three terms individually.

To circumvent this, we observe that to evaluate $f(|\psi\rangle, A, B)$, we do not need the ground state $|\psi\rangle$ itself, but only a classical description of its local reduced density matrices (a similar idea was used in [CS12] to verify the energy of a claimed product state proof against a local Hamiltonian in the setting of $\text{QMA}(2)$). Specifically, suppose Π consists of a k -local Hamiltonian H acting on n qubits. Then, the prover sends classical descriptions of k -qubit density matrices $\{\rho_S\}$ for each subset $S \subseteq [n]$ of size $|S| = k$, along with a QMA proof that the states $\{\rho_S\}$ are consistent with a global n -qubit pure state $|\psi\rangle$ (recall the problem of verifying consistency is QMA-complete [Liu06]). The verifier runs the QMA circuit for consistency, and assuming this check passes it uses the classical $\{\rho_S\}$ to classically verify that (1) $\langle\psi|H|\psi\rangle \leq \lambda(H) + \delta$ and (2) $f(|\psi\rangle, A, B) \geq a$ (since both of these depend only on the local states $\{\rho_S\}$).

□

6 $\text{PQMA}^{\text{[log]}}$ is in PP

We now restate and prove Theorem 1.3. Our approach is to develop a variant of the hierarchical voting scheme used in the proof of $\text{P}^{\text{NP}^{\text{[log]}}} \subseteq \text{PP}$ [BHW89] which uses the strong error reduction technique of Marriott and Watrous [MW05]. We also require a more involved analysis than present in [BHW89], since QMA is a class of promise problems, not decision problems.

Theorem 1.3. $\text{PQMA}^{\text{[log]}} \subseteq \text{PP}$.

Proof. Let Π be a P machine which makes $m = c \log n$ queries to an oracle for 2-LH, for $c \in O(1)$ and n the input size. Without loss of generality, we assume all queries involve Hamiltonians on M qubits (for M some fixed polynomial in n). Define $q := (M + 2)m$. We give a PQP computation simulating Π ; since $\text{PQP} = \text{PP}$ [Wat09], this suffices to show our claim. Let V denote the verification circuit for 2-LH. The PQP computation proceeds as follows (intuition to follow):

1. For i from 1 to m :
 - (a) Prepare $\rho = I/2^M \in \mathcal{D}((\mathbb{C}^2)^{\otimes M})$.
 - (b) Run V on the i th query Hamiltonian $H_{y_i}^{i, y_1 \dots y_{i-1}}$ (see Equation (4)) and proof ρ , and measure the output qubit in the standard basis. Set bit y_i to the result.
2. Let $y = y_1 \dots y_m$ be the concatenation of bits set in Step 1(b).
3. For i from 1 to $n^c - 1$:
 - (a) If $|y| < i$, then with probability $1 - 2^{-q}$, set $y = \#$, and with probability 2^{-q} , leave y unchanged.
4. If $y = \#$, output a bit in $\{0, 1\}$ uniformly at random. Else, run Π on query string y and output Π 's answer.

Intuition. In Step 1, one tries to determine the correct answer to query i by guessing a satisfying quantum proof for verifier V . Suppose for the moment that V has zero error, i.e. has completeness 1 and soundness 0, and that Π only makes valid queries. Then, if Step 1(b) returns $y_i = 1$, one knows with certainty that the query answer should be 1. And, if the correct answer to query i is 0, then Step 1(b) returns $y_i = 0$ with certainty. Thus, analogous to the classical case of an NP oracle (as done in [BHW89]), it follows that the lexicographically *largest* query string y^* obtainable by this procedure must be the (unique) correct query string (note that $y^* \neq 1^m$ necessarily, since a 1 in query i is only possible if query i is a YES instance of 2-LH). Thus, ideally one wishes to obtain y^* , simulate Π on y^* , and output the result. To this end, Step 3 ensures that among all values of $y \neq \#$, y^* is more likely to occur than all other $y \neq y^*$ combined. We now make this intuition rigorous (including in particular the general case where V is not zero-error and Π makes invalid queries).

Correctness. To analyze correctness of our PQP computation, it will be helpful to refine our partition of the set of query strings $\{0, 1\}^m$ into three sets:

- **(Correct query strings)** Let $A \subseteq \{0, 1\}^m$ denote the set of query strings which correspond to correctly answering each of the m queries. Note we may have $|A| > 1$ if invalid queries are made.
- **(Incorrect query strings)** Let $B \subseteq \{0, 1\}^m$ denote the set of query strings such that for any $y \in B$, any bit of y encoding an incorrect query answer is set to 0 (whereas the correct query answer would have been 1, i.e. we failed to “guess” a good proof for this query in Step 1).
- **(Strongly incorrect query strings)** Let $C = \{0, 1\}^m \setminus (A \cup B)$ denote the set of query strings such that for any $y \in C$, at least one bit corresponding to an incorrect query answer is set to 1 (whereas the correct query answer would have been 0). Such an error can only arise due to the bounded-error of our QMA verifier in Step 1(b).

Let Y be a random variable corresponding to the query string y obtained at the end of Step 3. To show correctness, we claim that it suffices to show that

$$\Delta := \Pr[Y \in A] - \Pr[Y \in B \cup C] > 0. \quad (13)$$

To see this, let p_1 , p_2 , and p_3 denote the probability that after Step 3, $y = \#$, $y \in A$, and $y \in B \cup C$, respectively. Then, $p_1 + p_2 + p_3 = 1$, and let $p_2 - p_3 = \Delta > 0$. Suppose now that the input to Π is a YES

instance. Then, our protocol outputs 1 with probability at least

$$\frac{p_1}{2} + p_2 = \frac{1 - p_2 - p_3}{2} + p_2 = \frac{1 + \Delta}{2} > \frac{1}{2}. \quad (14)$$

If the input is a NO instance, the protocol outputs 1 with probability at most $\frac{p_1}{2} + p_3 = \frac{1 - \Delta}{2} < \frac{1}{2}$. We hence have a QQP computation, as desired. We thus now show that Equation (13) holds.

To ease the presentation, we begin by making two assumptions (to be removed later): (i) V is zero-error and (ii) Π makes only valid queries. In this case, assumption (i) implies $C = \emptyset$ (i.e. all incorrect query strings belong to B), and (ii) implies A is a singleton (i.e. there is a unique correct query string y^*). Thus, here $\Delta = \Pr[Y \in A] - \Pr[Y \in B]$.

To begin, note that for any $y \in \{0, 1\}^m$, we have

$$\Pr[Y = y] = \Pr[y \text{ chosen in Step 2}] \cdot \left(\frac{1}{2^q}\right)^{(n^c-1)-|y|}, \quad (15)$$

where $|y|$ denotes the non-negative integer represented by string y . Let $\text{HW}(x)$ denote the Hamming weight of $x \in \{0, 1\}^m$. Since each query corresponds to a verifier on M proof qubits, we have for (the unique) $y^* \in A$ that

$$\Pr[y^* \text{ chosen in Step 2}] \geq 2^{-M \cdot \text{HW}(y^*)} \geq 2^{-Mm} \quad (16)$$

(recall from Section 2 that setting $\rho = I/2^M$ simulates “guessing” a correct proof with probability at least $1/2^M$). It follows by Equations (15) and (16) that

$$\begin{aligned} \Delta &\geq \left(\frac{1}{2^q}\right)^{(n^c-1)-|y^*|} \left[\frac{1}{2^{Mm}} - \sum_{y \in B} \left(\frac{1}{2^q}\right)^{|y^*|-|y|} \right], \\ &\geq \left(\frac{1}{2^q}\right)^{(n^c-1)-|y^*|} \left[\frac{1}{2^{Mm}} - (2^m) \left(\frac{1}{2^q}\right) \right], \\ &\geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} \right], \end{aligned} \quad (17)$$

where the first inequality follows since $\Pr[y \text{ chosen in Step 2}] \leq 1$, the second inequality since $y \in B$ if and only if $|y| < |y^*|$, and the third inequality since $q = (M + 2)m$. Thus, $\Delta > 0$ as desired.

Removing assumption (i). We now remove the assumption that V is zero error. In this case, A is still a singleton; let $y^* \in A$. We can now also have strongly incorrect query strings, i.e. $C \neq \emptyset$ necessarily. Assume without loss of generality that V acts on M proof qubits, and by strong error reduction [MW05] has completeness $c := 1 - 2^{p(n)}$ and soundness $s := 2^{p(n)}$, for p a polynomial to be chosen as needed. Then, since V can err, Equation (16) becomes

$$\begin{aligned} \Pr[y^* \text{ chosen in Step 2}] &\geq \left(\frac{c}{2^M}\right)^{\text{HW}(y^*)} (1 - s)^{m - \text{HW}(y^*)} \\ &= \frac{1}{2^M} e^{m \ln(1 - \frac{1}{2^p})} \\ &\geq \frac{1}{2^{Mm}} \left(1 - \frac{m}{2^p - 1}\right), \end{aligned} \quad (18)$$

where the equality follows by the definitions of c and s , and the second inequality by applying the Maclaurin series expansion of $\ln(1+x)$ for $|x| < 1$ and the fact that $e^t \geq 1+t$ for all $t \in \mathbb{R}$. Thus, the analysis of Equation (17) yields that

$$\Pr[Y \in A] - \Pr[Y \in B] \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p-1}\right], \quad (19)$$

i.e. the additive error introduced when assumption (i) is dropped scales roughly as 2^{-p} , where recall p can be set as needed. Note also that Equation (19) crucially holds for all $y \in B$ even with assumption (i) dropped since the analysis of Equation (17) used only the trivial bound $\Pr[y \text{ chosen in Step 2}] \leq 1$ for any $y \in B$.

Next, we upper bound the probability of obtaining $y \in C$ in Step 2. For any fixed $y \in C$, suppose the first bit on which y and y^* disagree is bit j . Then, bits j of y and y^* must be 1 and 0, respectively. This means 0 is the correct answer for query j . By the soundness property of V , the probability of obtaining 1 on query j (and hence that of obtaining y in Step 2) is at most 2^{-p} . Thus,

$$\Delta \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p-1}\right] - \frac{2^m}{2^p}. \quad (20)$$

We conclude that setting p to a sufficiently large fixed polynomial ensures $\Delta > 0$, as desired.

Removing assumption (ii). We now remove the assumption that Π only makes valid queries, which is the most involved step. Here, A is no longer necessarily a singleton. The naive approach would be to let y^* denote the *lexicographically largest* string in A , and attempt to run a similar analysis as before. Unfortunately, this no longer necessarily works for the following reason. For any invalid query i , we do not have strong bounds on the probability that V accepts in Step 1(b); in principle, this value can lie in the range $(2^{-p}, 1 - 2^{-p})$. Thus, running the previous analysis with the lexicographically largest $y^* \in A$ may cause Equation (20) to yield a negative quantity. This is because if bit i of y^* , denoted b , was set according to invalid query i , then the probability of obtaining bit b in query i may scale as $O(2^{-p})$; thus, both Equation (18) and Equation (19) would also scale as $O(2^{-p})$, and Equation (20) may be negative. We hence require a more delicate analysis.

We begin by showing the following lower bound.

Lemma 6.1. *Define $\Delta' := \Pr[Y \in A] - \Pr[Y \in B]$. Then,*

$$\Delta' \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p-1}\right].$$

Proof. We introduce the following definitions. For any string $y \in \{0, 1\}^m$, let $I_y \subseteq \{1, \dots, m\}$ denote the indices of all bits of y set by invalid queries. We call each such $i \in I_y$ a *divergence point*. Let $p_{y,i}$ denote the probability that (invalid) query i (defined given answers to queries 1 through $i-1$) outputs bit y_i , i.e. $p_{y,i}$ denotes the probability that at divergence point i , we go in the direction of bit y_i . We define the *divergence probability* of $y \in \{0, 1\}^m$ as $p_y = \prod_{i \in I_y} p_{y,i}$, i.e. p_y is the probability of answering all invalid queries as y did.

The proof now proceeds by giving an iterative process, $\Gamma(i)$, where $1 \leq i \leq |A|$ denotes the iteration number. Each iteration defines a 3-tuple $(y_{i-1}^*, y_i^*, B_{y_i^*}) \in \{0, 1\}^m \times \{0, 1\}^m \times \mathcal{P}(B)$, where $\mathcal{P}(X)$ denotes the power set of set X . Set

$$\Delta'_i := \Pr[Y \in \{y_1^*, \dots, y_i^*\}] - \Pr[Y \in B_{y_1^*} \cup \dots \cup B_{y_i^*}],$$

where it will be the case that $\{B_{y_i^*}\}_{i=1}^{|A|}$ is a partition of B . Thus, we have $\Delta' \geq \Delta'_{|A|}$, implying that a lower bound on $\Delta'_{|A|}$ suffices to prove our claim. We hence prove via induction that for all $1 \leq i \leq |A|$,

$$\Delta'_i \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p-1}\right].$$

The definition of process $\Gamma(i)$ is integrated into the induction proof below.

Base case ($i=1$). In this case y_0^* is undefined. Set y_1^* to the string in A with the largest divergence probability p_1^* . A key observation is that

$$p_1^* = \prod_{i \in I_{y_1^*}} p_{y_1^*, i} \geq 2^{-|I_{y_1^*}|}, \quad (21)$$

since at each divergence point i , at least one of the outcomes in $\{0, 1\}$ occurs with probability at least $1/2$. (It is important to note that queries are not being made to a QMA oracle here, but rather to a QMA verifier V with a maximally mixed proof as in Step 1(a). Whereas in the former case the output of the oracle on an invalid query does not have to consistently output a value with any particular probability, in the latter case, there is some fixed probability p with which V outputs 1 each time it is run on a fixed proof.) Finally, define $B_{y_1^*} := \{y \in B \mid |y| < |y_1^*|\}$.

Let k_* denote the number of divergence points of y_1^* (i.e. $k_* = |I_{y_1^*}|$), and k_0 (k_1) the number of zeroes (ones) of y_1^* arising from valid queries. Thus, $k_* + k_0 + k_1 = m$. Then, Equation (18) becomes

$$\Pr[y_1^* \text{ in Step 2}] \geq \left(\frac{c}{2^M}\right)^{k_1} (1-s)^{k_0} p_1^* \geq \left(\frac{1}{2^M}\right)^{k_1} \left(\frac{1}{2}\right)^{k_*} \left(1 - \frac{m-k_*}{2^p-1}\right) \geq \frac{1}{2^{Mm}} \left(1 - \frac{m}{2^p-1}\right), \quad (22)$$

where the second inequality follows from Equation (21), and the third since $k_* \geq 0$ and $k_1 + k_* \leq m$. Thus, Δ'_1 is lower bounded by the expression in Equation (19), completing the proof of the base case.

Inductive step. Assume the claim holds for $1 \leq i-1 < |A|$. We show it holds for i . Let y_{i-1}^* be the choice of y^* in the previous iteration $i-1$ of our process. Define $A_{y_i^*} := \{y \in A \mid |y| > |y_{i-1}^*|\}$. Partition $A_{y_i^*}$ into sets S_k for $k \in [m]$, such that S_k is the subset of strings in $A_{y_i^*}$ which agrees with y_{i-1}^* on the first $k-1$ bits, but disagrees on bit k . Note that if $S_k \neq \emptyset$, then bit k of y_{i-1}^* is 0 and bit k of any string in S_k is 1. For each $S_k \neq \emptyset$, choose an arbitrary representative $z_k \in S_k$, and define the *bounded* divergence probability

$$q_i(k) := \prod_{t \in I_{z_k}^{\leq k}} p_{z_k, t} \quad \text{where} \quad I_{z_k}^{\leq k} := \{t \in I_{z_k} \mid t \leq k\}.$$

Note that $q_i(k) > 0$ (since $S_k \neq \emptyset$). Else if $S_k = \emptyset$, set $q_i(k) = 0$. Let q_i^* denote the maximum such bounded divergence probability:

$$q_i^* = \max_{k \in [m]} q_i(k) \quad \text{and} \quad k_i^* = \arg \max_{k \in [m]} q_i(k). \quad (23)$$

Finally, let y_i^* be the query string in $S_{k_i^*}$ with the maximum divergence probability p_i^* (ties broken by choosing the lexicographically largest such query string). Observe that

$$p_i^* \geq q_i^* \cdot 2^{-|I_{y_i^*}| + |I_{y_i^*}^{\leq k_i^*}|}, \quad (24)$$

where the $2^{-|I_{y_i^*}| + |I_{y_i^*}^{\leq k}|}$ term arises from an argument similar to Equation (21) for all invalid queries of y_i^* after query k . Set $B_{y_i^*} := \{y \in B \mid |y_{i-1}^*| < |y| < |y_i^*|\}$. The following lemma will be useful.

Lemma 6.2. *For any $y \in B_{y_i^*}$, $\Pr[y \text{ chosen in Step 2}] \leq q_i^*$.*

Proof. Fix any $y \in B_{y_i^*}$. Since $|y| > |y_{i-1}^*|$, there must be an index k such that the k th bit of y is 1 and that of y_{i-1}^* is 0. Let k denote the first such index. Since $y \notin C$ (because $B_{y_i^*} \cap C = \emptyset$), it must be that query k (defined given bits $y_1 \cdots y_{k-1}$) is invalid. Thus, bit k is a divergence point of y_{i-1}^* , and there exists a correct query string $y' \in S_k$. By Equation (23), q_i^* was chosen as the maximum over all bounded diverge probabilities. Thus, $q_i^* \geq q_i(k)$, where recall $q_i(k)$ is the bounded divergence probability for S_k , where $y' \in S_k$. But since y and y' agree on bits 1 through k inclusive, we have $\Pr[y \text{ chosen in Step 2}] \leq \prod_{t \in I_y^{\leq k}} p_{y,t} = q_i(k)$, from which the claim follows. \square

To continue with the inductive step, again consider k_* , k_0 , and k_1 , now corresponding to y_i^* . Then, an argument similar to Equation (22) yields that $\Pr[y_i^* \text{ chosen in Step 2}]$ is at least

$$\left(\frac{c}{2^M}\right)^{k_1} (1-s)^{k_0} p_i^* \geq \left(\frac{1}{2^M}\right)^{k_1} \left(1 - \frac{m-k_*}{2^p-1}\right) q_i^* \left(\frac{1}{2}\right)^{|I_{y_i^*}| - |I_{y_i^*}^{\leq k_*}|} \geq \frac{q_i^*}{2^{Mm}} \left(1 - \frac{m}{2^p-1}\right), \quad (25)$$

where the first inequality follows from Equation (24), and the second since $|I_{y_i^*}| - |I_{y_i^*}^{\leq k_*}| \leq k_*$. Now, define $\zeta_i := \Pr[Y = y_i^*] - \Pr[Y \in B_{y_i^*}]$. Applying the argument of Equation (17), we have

$$\zeta_i \geq \left(\frac{1}{2^q}\right)^{(n^c-1)-|y_i^*|} \left[\frac{q_i^*}{2^{Mm}} \left(1 - \frac{m}{2^p-1}\right) - q_i^* \sum_{y \in B_{y_i^*}} \left(\frac{1}{2^q}\right)^{|y_i^*| - |y|} \right]$$

where the first q_i^* is due to Equation (25), and the second q_i^* to Lemma 6.2. Thus, similar to Equation (19),

$$\zeta_i \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{q_i^*}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p-1}\right] > 0.$$

Observing the recurrence that for all i , $\Delta'_i \geq \Delta'_{i-1} + \zeta_i$, unrolling this recurrence yields $\Delta'_i \geq \Delta_1$, which by the base case gives the claim of Lemma 6.1. \square

Combining Lemma 6.1 with the following lemma will yield our desired claim.

Lemma 6.3. $\Pr[Y \in C] \leq \frac{2^m}{2^p}$.

Proof. The argument is similar to that for Equation (20); we state it formally for clarity. Any $y \in C$ must have a bit j incorrectly set to 1, whereas the correct query answer (given bits 1 through $j-1$ of y) should have been 0. The probability of this occurring for bit j in Step 1(b) is at most 2^{-p} , by the soundness property of V . Since $|C| \leq 2^m$, the claim follows. \square

To complete the proof, we have that $\Pr[Y \in A] - \Pr[Y \in B \cup C]$ is lower bounded by

$$\Pr[Y \in A] - \Pr[Y \in B] - \Pr[Y \in C] \geq \left(\frac{1}{2^q}\right)^{(n^c-1)} \frac{1}{2^{Mm}} \left[1 - \frac{1}{2^m} - \frac{m}{2^p}\right] - \frac{2^m}{2^p},$$

which follows by Lemma 6.1 and Lemma 6.3. For sufficiently large fixed p , this quantity is strictly positive, yielding the claim of Theorem 1.3. \square

7 Estimating spectral gaps

We now restate and prove Theorem 1.4. We begin by defining SPECTRAL-GAP and UQMA.

Definition 7.1 (SPECTRAL-GAP(H, ϵ) (Ambainis [Amb14])). *Given a Hamiltonian H and a real number $\alpha \geq n^{-c}$ for n the number of qubits H acts on and $c > 0$ some constant, decide:*

- *If $\lambda_2 - \lambda_1 \leq \alpha$, output YES.*
- *If $\lambda_2 - \lambda_1 \geq 2\alpha$, output NO.*

where λ_2 and λ_1 denote the second and first smallest eigenvalues of H , respectively.

For clarity, if the ground space of H is degenerate, then we define its spectral gap as 0.

Definition 7.2 (Unique QMA (UQMA) (Aharonov *et al.* [ABOBS08])). *We say a promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in Unique QMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a quantum proof $|y\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:*

- *(Completeness) If $x \in A_{\text{yes}}$, then there exists a proof $|y\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ such that Q_n accepts $(x, |y\rangle)$ with probability at least $2/3$, and for all $|\hat{y}\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$ orthogonal to $|y\rangle$, Q_n accepts $(x, |\hat{y}\rangle)$ with probability at most $1/3$.*
- *(Soundness) If $x \in A_{\text{no}}$, then for all proofs $|y\rangle \in (\mathbb{C}^2)^{\otimes p(n)}$, Q_n accepts $(x, |y\rangle)$ with probability at most $1/3$.*

The main theorem of this section is the following.

Theorem 1.4. SPECTRAL-GAP is $\text{P}^{\text{UQMA}[\log]}$ -hard for 4-local Hamiltonians H under polynomial time Turing reductions (i.e. Cook reductions).

We remark that Ambainis [Amb14] showed that $\text{SPECTRAL-GAP} \in \text{P}^{\text{QMA}[\log]}$, and gave a claimed proof that SPECTRAL-GAP is $\text{P}^{\text{UQMA}[\log]}$ -hard for $O(\log)$ -local Hamiltonians under mapping reductions. ($\text{P}^{\text{UQMA}[\log]}$ is defined as $\text{P}^{\text{QMA}[\log]}$, except with a UQMA oracle in place of a QMA oracle.) As discussed in Section 1, however, Ambainis' proof of the latter result does not hold if the $\text{P}^{\text{UQMA}[\log]}$ machine makes invalid queries (which in general is the case). Here, we build on Ambainis' approach [Amb14] to show $\text{P}^{\text{UQMA}[\log]}$ -hardness of SPECTRAL-GAP under Turing reductions even when invalid queries are allowed, and we also improve the hardness to apply to $O(1)$ -local Hamiltonians.

For this, we may assume that all calls to the UQMA oracle Q are for an instance (H, a, b) of the Unique-Local Hamiltonian Problem (U-LH) [Amb14]: Is the ground state energy of H at most ϵ with all other eigenvalues at least 3ϵ (YES case), or is the ground state energy at least 3ϵ (NO case), for $\epsilon \geq 1/\text{poly}(n)$? We begin by showing the following modified version of Lemma 3.2 tailored to UQMA (instead of QMA).

Lemma 7.3. *For any $x \in \{0, 1\}^m$, let \hat{x} denote its unary encoding. Then, for any $\text{P}^{\text{UQMA}[\log]}$ circuit U acting on n bits and making m queries to a UQMA oracle, there exists a 4-local Hamiltonian H acting on space $(\mathbb{C}^2)^{\otimes 2^m-1} \otimes \mathcal{Y}$ such that there exists a correct query string $x = x_1 \cdots x_m$ such that:*

1. *The unique ground state of H lies in subspace $|\hat{x}\rangle\langle\hat{x}| \otimes \mathcal{Y}$.*
2. *The spectral gap of H is at least $(\epsilon - \delta)/4^m$ for inverse polynomial ϵ, δ with $\epsilon - \delta \geq 1/\text{poly}(n)$.*

3. For all strings $x' \in \{0, 1\}^m$, H acts invariantly on subspace $|\hat{x}'\rangle\langle\hat{x}'| \otimes \mathcal{Y}$.

Proof. As done in [Amb14], we begin with $O(\log)$ -local Hamiltonian

$$H' = \sum_{i=1}^m \frac{1}{4^{i-1}} \sum_{y_1, \dots, y_{i-1}} \bigotimes_{j=1}^{i-1} |y_j\rangle\langle y_j|_{\mathcal{X}_j} \otimes G'_{y_1 \dots y_{i-1}}, \quad (26)$$

where we define

$$G'_{y_1 \dots y_{i-1}} := |0\rangle\langle 0|_{\mathcal{X}_i} \otimes A_{\mathcal{Y}_i} + |1\rangle\langle 1|_{\mathcal{X}_i} \otimes H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}} \quad (27)$$

with A any fixed 2-local Hermitian operator with unique ground state of eigenvalue 2ϵ and spectral gap ϵ . Our approach is intuitively now as follows. We first run a *query validation* phase, in which we modify H' to obtain a new Hamiltonian H'' by replacing “sufficiently invalid” queries $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$ with high-energy dummy queries. This creates the desired spectral gap. We then apply the technique of Lemma 3.2 to reduce the locality of H'' , obtaining a 4-local Hamiltonian H , as desired. Note that our proof shows *existence* of H ; unlike Lemma 3.2, however, it is not clear how to construct H in polynomial-time given H' , as detecting invalid UQMA queries with a P machine seems difficult.

The query validation phase proceeds as follows. Consider any $G'_{y_1 \dots y_{i-1}}$ whose spectral gap is at most $\epsilon - \delta$, for some fixed δ satisfying $\epsilon - \delta \geq 1/\text{poly}(n)$. We claim this implies $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$ is an invalid query. For if $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$ were a valid YES query, then $\lambda(G'_{y_1 \dots y_{i-1}}) \leq \epsilon$ and $\lambda_2(G'_{y_1 \dots y_{i-1}}) = 2\epsilon$ (by the $|0\rangle\langle 0|$ block of $G'_{y_1 \dots y_{i-1}}$, and since a valid query to U-LH has a spectral gap of 2ϵ), where $\lambda_2(X)$ is the second-smallest eigenvalue of operator X . Conversely, if $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$ were a valid NO query, then $\lambda(G'_{y_1 \dots y_{i-1}}) = 2\epsilon$ (by the $|0\rangle\langle 0|$ block of $G'_{y_1 \dots y_{i-1}}$) and $\lambda_2(G'_{y_1 \dots y_{i-1}}) \geq 3\epsilon$. Thus, $H_{\mathcal{Y}_i}^{i, y_1 \dots y_{i-1}}$ corresponds to an invalid query. Replace each such $G'_{y_1 \dots y_{i-1}}$ with

$$G_{y_1 \dots y_{i-1}} := |0\rangle\langle 0|_{\mathcal{X}_i} \otimes A_{\mathcal{Y}_i} + |1\rangle\langle 1|_{\mathcal{X}_i} \otimes 3\epsilon I \quad (28)$$

in H' , denoting the new Hamiltonian as H'' . Two remarks: First, the validation phase does not catch *all* invalid queries, but only those which are “sufficiently far” from being valid. Second, setting $\delta \in \Omega(1/\text{poly}(n))$ (as opposed to, say, $1/\exp(n)$) is required for our proof of Theorem 1.4 later.

We now show correctness. Observe first that for any “sufficiently invalid” query i , replacing $G'_{y_1 \dots y_{i-1}}$ with $G_{y_1 \dots y_{i-1}}$ in the validation phase “forces” query i to become a valid NO query. Thus, henceforth in this proof, a query string which answers YES (i.e. $|1\rangle$) to query i is considered incorrect with respect to H'' . Crucially, if a string x is a correct query string for H'' , then it is also a correct query string for H' . The converse is false; nevertheless, H'' has at least one correct query string (since any sufficiently invalid query would have allowed both $|0\rangle$ and $|1\rangle$ as answers), which suffices for our purposes.

To begin, as in the proof of Lemma 3.1, observe that H'' is block-diagonal with respect to register $\bigotimes_{i=1}^m \mathcal{X}_i$. Let $x \in \{0, 1\}^m$ denote a correct query string which has minimal energy among all *correct* query strings against H'' , and for any $y \in \{0, 1\}^m$, define λ_y as the smallest eigenvalue in block \mathcal{H}_y . A similar analysis to that of Lemma 3.1 shows that for any incorrect query string y , $\lambda_y \geq \lambda_x + \epsilon/4^m$. This is because replacing the term $2\epsilon I$ in $M_{y_1 \dots y_{i-1}}$ from Lemma 3.1 with A in $G_{y_1 \dots y_{i-1}}$ here preserves the property that answering NO on query i yields minimum energy 2ϵ .

We now argue that x is in fact *unique*, and all other eigenvalues of H'' corresponding to correct query strings have energy at least $\lambda_x + (\epsilon - \delta)/4^m$. There are two cases to consider: Eigenvalues arising from different query strings, and eigenvalues arising from the same query string.

Case 1: Eigenvalues from different query strings. Let $y = y_1 \cdots y_m$ be a correct query string for H'' . Since both x and y are correct strings, there must exist an invalid query i where $x_i \neq y_i$. First consider the case where $G'_{y_1 \cdots y_{i-1}}$ has spectral gap at most $\epsilon - \delta$. Then, after the validation phase, query i is replaced with a valid NO query $G_{y_1 \cdots y_{i-1}}$. Thus, whichever of x or y has a 1 as bit i is an incorrect string for H'' , and from our previous analysis has energy at least $\lambda_x + \epsilon/4^m$ against H'' . (This, in particular, implies $x_i = 0$ and $y_i = 1$.) Alternatively, suppose $G'_{y_1 \cdots y_{i-1}} = G_{y_1 \cdots y_{i-1}}$ has spectral gap at least $\epsilon - \delta$. By construction of A (which has spectral gap ϵ), it follows that $\lambda(H_{\mathcal{Y}_i}^{i, y_1 \cdots y_{i-1}})$ is at most $\epsilon + \delta$ or at least $3\epsilon - \delta$. In other words, query i is “approximately” valid, and y must be “approximately” incorrect on query i . A similar analysis as for Lemma 3.1 hence yields $\lambda_y \geq \lambda_x + (\epsilon - \delta)/4^m$.

Case 2: Eigenvalues from the same query string. In block \mathcal{H}_x , H'' is equivalent to operator

$$\sum_{i=1}^m \frac{1}{4^{i-1}} B_{x_1 \cdots x_{i-1}},$$

where $B_{x_1 \cdots x_{i-1}} = A$ if $x_i = 0$ and $B_{x_1 \cdots x_{i-1}}$ can equal either $H_{\mathcal{Y}_i}^{i, y_1 \cdots y_{i-1}}$ or $3\epsilon I$ (depending on how the validation phase proceeded) if $x_i = 1$. In particular, $B_{x_1 \cdots x_{i-1}}$ acts non-trivially only on space \mathcal{Y}_i and has spectral gap at least $\epsilon - \delta$. Clearly, the ground state of H'' of form $|\hat{x}\rangle |\psi\rangle$ obtains the smallest eigenvalue of each term $B_{x_1 \cdots x_{i-1}}$, and the first excited state (corresponding to the second eigenvalue) of H'' must take on the first excited state of at least one $B_{x_1 \cdots x_{i-1}}$, implying a spectral gap of at least $(\epsilon - \delta)/4^m$, as claimed.

Finally, the approach of Lemma 3.2 allows us to convert $O(\log)$ -local H'' to 4-local H . \square

Proof of Theorem 1.4. As done in [Amb14], we start with the Hamiltonian H' from Equation (26). In [Amb14], it was shown (Section A.3, Claim 2) that if all query Hamiltonians $H_{\mathcal{Y}_i}^{i, y_1 \cdots y_{i-1}}$ correspond to valid UQMA queries, H' has a unique ground state and spectral gap at least $\epsilon/4^m$. When invalid queries are allowed, however, the spectral gap of H' can vanish, invalidating the $\text{P}^{\text{UQMA}[\log]}$ -hardness proof of [Amb14]. Thus, we require a technique for identifying invalid queries and “removing them” from H' .

Unfortunately, it is not clear how a P machine alone can achieve such a “property testing” task of checking if a query is sufficiently invalid. However, the key observation is that an oracle Q for SPECTRAL GAP can help. A bit of care is required here; naively, one might check if each query $H_{\mathcal{Y}_i}^{i, y_1 \cdots y_{i-1}}$ has a spectral gap using Q , since in the YES case, this must hold. However, it is quickly seen that even invalid queries can have a spectral gap.

Instead, we proceed as follows. Given an arbitrary $\text{P}^{\text{UQMA}[\log]}$ circuit U acting on n bits, construct $O(\log(n))$ -local H' from Equation (26). For each term $G'_{y_1 \cdots y_{i-1}}$ appearing in H' , perform binary search using $O(\log n)$ queries to Q to obtain an estimate Δ for the spectral gap of $G'_{y_1 \cdots y_{i-1}}$ to within sufficiently small but fixed additive error $\delta \in 1/\text{poly}(n)$. (A similar procedure involving a QMA oracle is used in Ambainis’ proof of containment of $\text{APX-SIM} \in \text{P}^{\text{QMA}[\log]}$ to estimate the smallest eigenvalue of a local Hamiltonian; we hence omit further details here.) As done in the proof of Lemma 7.3, if $\Delta \leq \epsilon - \delta$, we conclude $H_{\mathcal{Y}_i}^{i, y_1 \cdots y_{i-1}}$ is “sufficiently invalid”, and replace $G'_{y_1 \cdots y_{i-1}}$ with $G_{y_1 \cdots y_{i-1}}$ from Equation (28). Following the construction of Lemma 7.3, we hence can map H' to a 4-local Hamiltonian H such that H has a unique ground state and spectral gap $(\epsilon - \delta)/4^m$, and the ground state of H corresponds to a correct query string for H' . Note that implementing the mapping from H' to H requires polynomially many queries to the oracle, hence yielding a polynomial time *Turing* reduction.

Next, following [Amb14], let $T := \sum_{y_1 \cdots y_m} \bigotimes_{i=1}^m |y_i\rangle \langle y_i| \in \text{L}(\mathcal{Y})$, where we sum over all query strings $y_1 \cdots y_m$ which cause U to output 0. Unlike [Amb14], as done in Lemma 3.2, we apply Kitaev’s

unary encoding trick [KSV02] and implicitly encode the query strings in T in unary. (We remark the term H_{stab} contained in H will enforce the correct unary encoding in register \mathcal{X}). Finally, introduce a single-qubit register \mathcal{B} , and define

$$H_{\text{final}} := I_{\mathcal{B}} \otimes H_{\mathcal{X},\mathcal{Y}} + 4\epsilon |0\rangle\langle 0|_{\mathcal{B}} \otimes T_{\mathcal{X}} \otimes I_{\mathcal{Y}}.$$

The claim now follows via an analysis similar to [Amb14]. Let $|\psi\rangle_{\mathcal{X},\mathcal{Y}}$ denote the unique ground state of H , whose \mathcal{X} register contains the (unary encoding of) a correct query string for U . If U accepts, then $|i\rangle_{\mathcal{B}} \otimes |\psi\rangle_{\mathcal{X},\mathcal{Y}}$ for $i \in \{0, 1\}$ are degenerate ground states of H_{final} , implying H_{final} has no spectral gap. Conversely, if U rejects, observe that the smallest eigenvalue of H_{final} lies in the $|1\rangle_{\mathcal{B}}$ block of H_{final} . This is because H_{final} is block-diagonal with respect to register \mathcal{X} , and we have from the proof of Lemma 3.2 that $\lambda(H) < 3\epsilon$. Restricted to this $|1\rangle_{\mathcal{B}}$ block, the spectral gap of H_{final} is at least $(\epsilon - \delta)/4^m$ by Lemma 7.3. Alternatively, restricted to the $|0\rangle_{\mathcal{B}}$ block, any correct query string in \mathcal{X} leads to spectral gap at least 4ϵ (by construction of T , since U outputs 0 in this case), and any incorrect query string in \mathcal{X} leads to spectral gap at least $(\epsilon - \delta)/4^m$ by Lemma 7.3. Hence, H_{final} has an inverse polynomial spectral gap, as desired. \square

8 Conclusions and open questions

We have studied the complexity of physical problems involving local Hamiltonians beyond the paradigm of estimating ground state energies. In this setting, we showed that measuring even a 1-local observable against a 5-local Hamiltonian’s ground state (i.e. APX-SIM) is $\text{PQMA}^{[\log]}$ -complete, and so is “slightly harder” than QMA. Similarly, we showed that estimating a two-point correlation function (i.e. APX-2-CORR) is $\text{PQMA}^{[\log]}$ -complete. We upper bounded the complexity of $\text{PQMA}^{[\log]}$ by showing it is contained in PP. Finally, we built on an approach of Ambainis [Amb14] to show $\text{P}^{\text{UQMA}^{[\log]}}$ -hardness under Turing reductions of determining the spectral gap of a local Hamiltonian.

Although we resolve one of the open questions from [Amb14], there are others we leave open, along with some new ones. Do our results for APX-SIM and APX-2-CORR still hold for 2-local Hamiltonians, or (say) local Hamiltonians on a 2D lattice? Do such results also hold for specific Hamiltonian models of interest, such as the Heisenberg anti-ferromagnet on spin-1/2 particles? For example, when large coefficients for each local constraint are allowed, determining the ground state of the latter is QMA-complete [CM13, PM15]. Can SPECTRAL-GAP be shown to be either $\text{P}^{\text{UQMA}^{[\log]}}$ -complete or $\text{PQMA}^{[\log]}$ -complete (recall SPECTRAL-GAP is in $\text{PQMA}^{[\log]}$, and [Amb14] and our work together show $\text{P}^{\text{UQMA}^{[\log]}}$ -hardness)? What is the relationship between $\text{PQMA}^{[\log]}$ and $\text{P}^{\text{UQMA}^{[\log]}}$? Finally, exploring the landscape of quantum Hamiltonian complexity beyond the confines of QMA has helped to characterize the complexity of physical tasks beyond estimating ground state energies — what other relevant tasks are complete for $\text{PQMA}^{[\log]}$, or for other classes beyond QMA?

Acknowledgements

We thank Xiaodi Wu for stimulating discussions which helped motivate this project, including the suggestion to think about estimating two-point correlation functions (which arose via discussions with Aram Harrow, whom we also thank). We also thank Andris Ambainis and Norbert Schuch for helpful discussions, and remark that they independently conceived of some of the ideas behind Lemma 3.2 and Theorem 1.1, respectively (private communication). Part of this work was completed while SG was supported by a Government of Canada NSERC Banting Postdoctoral Fellowship and the Simons Institute for the Theory of Computing at UC Berkeley. SG acknowledges support from NSF grant CCF-1526189.

References

- [ABOBS08] D. Aharonov, M. Ben-Or, F. Brandão, and O. Sattath. The pursuit for uniqueness: Extending Valiant-Vazirani theorem to the probabilistic and quantum settings. Available at arXiv.org e-Print quant-ph/0810.4840v1, 2008.
- [Amb14] A. Ambainis. On physical problems that are slightly more difficult than QMA. In *Proceedings of 29th IEEE Conference on Computational Complexity (CCC 2014)*, pages 32–43, 2014.
- [AN02] D. Aharonov and T. Naveh. Quantum NP - A survey. Available at arXiv.org e-Print quant-ph/0210077v1, 2002.
- [BFS11] B. Brown, S. Flammia, and N. Schuch. Computational difficulty of computing the density of states. *Physical Review Letters*, 104:040501, 2011.
- [BHW89] R. Beigel, L. A. Hemachandra, and G. Wechsung. On the power of probabilistic polynomial time: $P^{NP[\log]} \subseteq PP$. In *Proceedings of the 4th IEEE Conference on Structure in Complexity Theory*, pages 225–227, 1989.
- [Boo14] A. D. Bookatz. QMA-complete problems. *Quantum Information & Computation*, 14(5–6), 2014.
- [CM13] T. Cubitt and A. Montanaro. Complexity classification of local hamiltonian problems. Available at arXiv.org e-Print quant-ph/1311.3161, 2013.
- [Coo72] S. Cook. The complexity of theorem proving procedures. In *Proceedings of the 3rd ACM Symposium on Theory of Computing (STOC 1972)*, pages 151–158, 1972.
- [CS12] A. Chailloux and O. Sattath. The complexity of the separable Hamiltonian problem. In *Proceedings of 27th IEEE Conference on Computational Complexity (CCC 2012)*, pages 32–41, 2012.
- [Gha13] S. Gharibian. *Approximation, proof systems, and correlations in a quantum world*. PhD thesis, University of Waterloo, 2013. Available at arXiv.org e-Print quant-ph/1301.2632.
- [GHLS14] Sevag Gharibian, Yichen Huang, Zeph Landau, and Seung Woo Shin. Quantum Hamiltonian complexity. *Foundations and Trends in Theoretical Computer Science*, 10(3):159–282, 2014.
- [Gil77] J. Gill. Computational complexity of probabilistic Turing machines. *SIAM Journal on Computing*, 6(4):675–695, 1977.
- [GK12] S. Gharibian and J. Kempe. Hardness of approximation for quantum problems. In *Proceedings of 39th International Colloquium on Automata, Languages and Programming (ICALP 2012)*, pages 387–398, 2012.
- [Gol06] O. Goldreich. On promise problems: A survey. *Theoretical Computer Science*, 3895:254–290, 2006.
- [GS15] S. Gharibian and J. Sikora. Ground state connectivity of local Hamiltonians. In *Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming (ICALP 2015)*, pages 617–628, 2015.

- [Kar72] R. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103. New York: Plenum, 1972.
- [KKR06] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.
- [KSV02] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.
- [KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the 32nd ACM Symposium on Theory of Computing (STOC 2000)*, pages 608–617, 2000.
- [Lev73] L. Levin. Universal search problems. *Problems of Information Transmission*, 9(3):265–266, 1973.
- [Liu06] Y.-K. Liu. Consistency of local density matrices is QMA-complete. In *Lecture Notes in Computer Science*, volume 4110, pages 438–449, 2006.
- [MW05] C. Marriott and J. Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.
- [NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [PM15] S. Piddock and A. Montanaro. The complexity of antiferromagnetic interactions and 2d lattices. Available at arXiv.org e-Print quantph/1506.04014, 2015.
- [SZ] Y. Shi and S. Zhang. Note on quantum counting classes. Available at <http://www.cse.cuhk.edu.hk/syzhang/papers/SharpBQP.pdf>.
- [Vya03] M. Vyalyi. QMA=PP implies that PP contains PH. *Electronic Colloquium on Computational Complexity*, 2003.
- [Wat09] J. Watrous. *Encyclopedia of Complexity and System Science*, chapter Quantum Computational Complexity. Springer, 2009.